

IN THE DISTRICT COURT OF BECKHAM COUNTY
STATE OF OKLAHOMA

BECKHAM COUNTY
FILED
NOV 22 2024
DONNA HOWELL, COURT CLERK
BY _____ DEPUTY

CHRISTOPHER EVANS, on behalf of
himself and on behalf of all others
similarly situated,

Plaintiff,

v.

FARMERS UNION HOSPITAL
ASSOCIATION d/b/a GREAT
PLAINS REGIONAL MEDICAL
CENTER,

Defendant.

Case No.

CJ-24-123

Judge:

Dirickson

JURY TRIAL DEMANDED

CLASS ACTION PETITION

Plaintiff Christopher Evans (“Plaintiff”), individually and on behalf of all other similarly situated individuals (the “Class” or “Class Members,” as defined below), by and through his undersigned counsel, files this Class Action Petition against Farmers Union Hospital Association d/b/a Great Plains Regional Medical Center (“GPRMC” or “Defendant”) and alleges the following based on personal knowledge of facts, upon information and belief, and based on the investigation of his counsel as to all other matters.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against GPRMC for its negligent failure to protect and safeguard Plaintiff’s and Class Members’ highly sensitive personally identifiable information (“PII”) and protected health information (“PHI”) (together, “Private Information”), culminating in a massive and preventable data breach (the “Data Breach” or “Breach”).¹

¹ See <https://gprmc-ok.com/notice-of-security-incident/>.

2. As a result of GPRMC's negligence and deficient data security practices, cybercriminals easily infiltrated GPRMC's inadequately protected computer systems and **stole** the Private Information of Plaintiff and Class Members—at least **133,149 individuals**.²

3. According to GPRMC, on or around September 5 through September 8, 2024, it became aware of potential unauthorized access to an employee email account.

4. After an investigation, on September 8, 2024, GPRMC determined highly confidential PHI and PII may have been accessed during the Breach, but did not publicly disclose the Breach to Plaintiff until November 7, 2024.³

5. GPRMC admits point-blank that “We learned that the bad actor copied some of those files. We quickly restored our systems and returned to normal operations, but we also determined that a limited amount of patient information was not recoverable.”⁴

6. The stolen information varies by individual, but generally included one or more of the following: name, demographic information Social Security Number, driver's license number, health insurance information, and/or clinical treatment information, such as diagnosis and medication information (collectively, “Private Information”).⁵

7. According to information and belief, the victims of the Data Breach include current and former GPRMC patients.

8. To date, there is no indication that GPRMC has made any attempt to recover Plaintiff's and Class Members' Private Information.

² See https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

³ *Id.*; Ex. 1 (Notice Letter).

⁴ *Id.*; Ex. 1 (Notice Letter).

9. There is no question Plaintiff's and Class Members' Private Information is in the hands of cybercriminals who will use the stolen Private Information for nefarious purposes for the rest of their lives.

10. Due to GPRMC's negligent failure to secure and protect Plaintiff's and Class Members' Private Information, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

11. Now, and for the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft will have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach.

12. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminution of the value of their Private Information, loss of privacy, and additional damages as described below.

13. Plaintiff brings this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, injunctive and declaratory relief, reasonable attorneys' fees and costs, and all other remedies this Court deems just and proper.

II. THE PARTIES

14. Plaintiff **Christopher Evans** is an individual domiciled in the State of Oklahoma. Plaintiff Evans received a letter informing him he was a victim of the Data Breach a "Notice

Letter” or “Notice of Data Breach Letter” dated November 7, 2024, informing him that his name, demographic information, Social Security Number, driver’s license number, health insurance information, and/or clinical treatment information, were subject to unauthorized access.⁶

15. Defendant **GPRMC** is a domestic not for profit corporation with its principal place of business at 1801 W. 3rd Street, Elk City, Oklahoma, 73644. GPRMC’s registered agent is Demi Hall, located at 1801 W. 3rd Street, Elk City, Oklahoma, 73644.

III. JURISDICTION AND VENUE

16. This Court is a court of general jurisdiction that has jurisdiction over the subject matter of this action by virtue of Okla. Const. Art. 7 § 7 and enacting legislation.

17. This Court has personal jurisdiction over GPRMC because GPRMC is a domestic not for profit corporation with members and managers located in this District, has substantial contacts with Beckham County, Oklahoma and purposefully availed itself of the laws and Courts in Beckham County, Oklahoma.

18. Venue is proper in Beckham County, Oklahoma by virtue of Okla. Stat. Ann. Tit. 12 § 134, because Defendant is a not-for-profit corporation created by the laws of Oklahoma and provides services to patients in Beckham County, Oklahoma, and conducts a substantial amount of business in Beckham County, Oklahoma. Additionally, a substantial part of the events giving rise to this action occurred in Beckham County, Oklahoma. Defendant also maintains Plaintiff’s and Class Members’ Private Information in Beckham County, Oklahoma, and has caused harm to Plaintiff and Class Members located in Beckham County, Oklahoma.

IV. FACTUAL ALLEGATIONS

A. GPRMC Collected Plaintiff’s and Class Members’ Private Information.

⁶ See Ex. 1.

19. Built in 1929, GPRMC is a healthcare provider located at 1801 W. 3rd Street, Elk City, Oklahoma 73644.14101⁷

20. GPRMC provides comprehensive, cost effective healthcare to patients.⁸

21. GPRMC could have afforded to implement adequate data security prior to the Data Breach but deliberately chose not to.

22. In the ordinary course of its business, GPRMC receives and stores the Private Information of thousands of patients and employees, including Plaintiff and Class Members.

23. GPRMC solicits, collects, uses, and derives a benefit from Plaintiff's and Class Members' Private Information.

24. GPRMC uses the Private Information it solicits, collects, and stores to provide healthcare services, making a profit therefrom.

25. GPRMC would be unable to engage in its regular business activities without collecting and aggregating Private Information it knows and understands to be sensitive and confidential.

26. Class Members who are current and former patients of GPRMC paid GPRMC for medical services. GPRMC promised data security to its patients as part of these medical services and part of this payment should have been specifically allocated to data security.

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

⁷ <https://gprmc-ok.com/history/>.

⁸ <https://gprmc-ok.com/services/>.

28. GPRMC failed to implement adequate data security measures to protect Plaintiff's and Class Members' Private Information, resulting in a devastating data breach that affected over 133,149 individuals.

B. GPRMC's Massive and Preventable Data Breach.

29. According to GPRMC's notice:⁹

On September 8, 2024, we suffered a ransomware attack on our computer system. We secured our systems and began an investigation with the help of a cybersecurity firm. This investigation showed that an unknown person accessed and encrypted files on our systems between September 5, 2024 and September 8, 2024. We learned that the bad actor copied some of those files. We quickly restored our systems and returned to normal operations, but we also determined that a limited amount of patient information was not recoverable.

The patient information varied by individual, but may have included: name, demographic information, health insurance information, clinical treatment information, such as diagnosis and medication information, driver's license number, and/or in some instances, Social Security number.

30. Despite learning of the Data Breach on September 8, 2024, GPRMC inexplicably waited to notify Plaintiff and the Class of the Data Breach until on or around November 7, 2024, when it began sending Notice of Data Breach Letters to victims of the Data Breach.¹⁰

31. The Notice Letter provided by GPRMC amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members, with any degree of specificity, of critical facts

⁹ <https://gprmc-ok.com/notice-of-security-incident/>

¹⁰ *See id.*

concerning the Data Breach. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

32. GPRMC failed to take the necessary precautions required to safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access and exploitation.

33. GPRMC also failed to timely notify Plaintiff and Class Members of the Data Breach.

34. GPRMC's actions represent a flagrant disregard of the rights of Plaintiff and the Class, both as to privacy and property.

35. As such, Plaintiff and the Class continue to be at an imminent and impending risk of identity theft and fraud.

C. Cybercriminals Will Use Plaintiff's and Class Members' Private Information to Defraud them.

36. Private Information is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

37. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.¹¹

38. For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, obtain medical services, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal

¹¹ *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (last visited November 21, 2024).

government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.¹²

39. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

40. Medical-related identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, “medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013[,]” which is more than identity thefts involving banking and finance, the government and the military, or education.¹³

41. “Medical records are a gold mine for criminals—they can access a patient’s name, DOB, Social Security and insurance numbers, and even financial information all in one place.”¹⁴ A complete identity theft kit that includes health insurance credentials may be worth up to \$1,000 on the black market.¹⁵

42. When cybercriminals manage to steal health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Plaintiff and Class Members are exposed.

¹² See, e.g., Nikkita Walker, *What Can You Do With Your Social Security Number*, CREDIT.COM (Oct. 19, 2023), <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

¹³ Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), <https://khn.org/news/rise-of-identity-theft/>.

¹⁴ *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, New Ponemon Study Shows, IDX (May 14, 2015) <https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat..>

¹⁵ *Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015*, PRICEWATERHOUSECOOPERS (Sept. 30, 2014), <https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf>.

43. Social Security numbers are particularly sensitive pieces of personal information.

As the Consumer Federation of America explains:

Social Security number. *This is the most dangerous type of personal information in the hands of identity thieves because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It’s hard to change your Social Security number and it’s not a good idea because it is connected to your life in so many ways.*¹⁶

(Emphasis added.)

44. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.¹⁷

45. The Data Breach at issue here was targeted and financially motivated, as the only reason cybercriminals go through the trouble of hacking companies like GPRMC is to steal the highly sensitive information they maintain, which can be exploited and sold for use in the kinds of criminal activity described herein.

46. A Social Security number, date of birth, and full name can sell for \$60 to \$80 on the digital black market.¹⁸

47. PHI is even more valuable on the black market than PII.¹⁹

¹⁶ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

¹⁷ *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), <https://www.gao.gov/products/gao-07-737>.

¹⁸ Michael Kan, *Here’s How Much Your Identity Goes for on the Dark Web*, PGMAG (Nov. 15, 2017), <https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web>.

¹⁹ *Data Breaches: In the Healthcare Sector*, CENTER FOR INTERNET SECURITY, <https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector> (last visited April 11, 2024).

48. According to the Center for Internet Security, “[t]he average cost of a data breach incurred by a non-healthcare related agency, per stolen record, is \$158. For healthcare agencies the cost is an average of \$355. Credit card information and PII sell for \$1-\$2 on the black market, but PHI can sell for as much as \$363 according to the Infosec Institute. This is because one’s personal health history, including ailments, illnesses, surgeries, etc., can’t be changed, unlike credit card information or Social Security Numbers.”²⁰

49. “PHI is valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim’s medical conditions or victim settlements. It can also be used to create fake insurance claims, allowing for the purchase and resale of medical equipment. Some criminals use PHI to illegally gain access to prescriptions for their own use or resale.”²¹

50. Identity theft experts advise victims of data breaches: “[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web.”²²

51. These risks are both certainly impending and substantial. As the Federal Trade Commission (“FTC”) has reported, if hackers get access to PII, **they will use it.**²³

52. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data

²⁰ *Id.*

²¹ *Id.*

²² *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

²³ Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), <https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info>.

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.²⁴

53. For instance, with a stolen Social Security number, which is part of the Private Information compromised in the Data Breach, criminals can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.²⁵

54. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.²⁶

55. GPRMC made a limited offering of identity monitoring to Plaintiff and the Class. Such coverage is woefully inadequate and will not fully protect Plaintiff and the Class from the damages and harm caused by GPRMC's negligent failure to secure and protect their Private Information.

56. The unfortunate truth is the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs and when it is discovered, and also between when Private Information is stolen and when it is used.

57. Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to GPRMC's negligence.

²⁴ *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), <https://www.gao.gov/products/gao-07-737> (emphasis added).

²⁵ See Nikkita Walker, *What Can Someone Do with Your Social Security Number?*, CREDIT.COM (Oct. 19, 2023), <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

²⁶ *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), <https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf>.

58. Furthermore, identity monitoring services only alert someone to the fact that they have already been the victim of identity theft—it does not prevent identity theft.²⁷

59. Nor can an identity monitoring service remove personal information from the dark web.²⁸

60. “The people who trade in stolen personal information [on the dark web] won’t cooperate with an identity theft service or anyone else, so it’s impossible to get the information removed, stop its sale, or prevent someone who buys it from using it.”²⁹

61. As a direct and proximate result of the Data Breach, Plaintiff and the Class have been damaged and placed at an imminent and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and medical records for unauthorized activity for years to come.

62. Even more serious is the identity restoration that Plaintiff and other Class Members must go through, which can require spending countless hours filing police reports, filling out IRS forms, completing Federal Trade Commission checklists and Department of Motor Vehicle driver’s license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

²⁷ See Kayleigh Kulp, *Credit monitoring services may not be worth the cost*, CNBC (Nov. 30, 2017, 9:00 AM), <https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html>.

²⁸ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

²⁹ *Id.*

63. Plaintiff and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

- a. Actual identity theft;
- b. Trespass, damage to, and theft of their personal property, including their Private Information;
- c. Improper disclosure and theft of their Private Information;
- d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;
- e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cybercriminals have their Private Information;
- f. Ascertainable losses in the form of time taken to respond to identity theft, including lost opportunities and lost wages from uncompensated time off from work;
- g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;
- h. Ascertainable losses in the form of diminution of the value of Plaintiff's and Class Members' Private Information, for which there is a well-established and quantifiable national and international market;
- i. The loss of use of and access to their credit, accounts, and/or funds;
- j. Damage to their credit due to fraudulent use of their Private Information; and/or
- k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

64. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches through the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiff's and Class Members' Private Information.

65. Plaintiff and Class Members also have an interest in ensuring that their Private Information is removed from all GPRMC servers, systems, and files.

66. The notice provided by GPRMC acknowledged that the Data Breach would cause harm to affected individuals and that financial harm would likely occur, stating:³⁰

We are mailing letters to affected patients and offering free credit monitoring to those whose Social Security number or driver's license number may have been involved. If you believe you are affected by this incident and do not receive a letter by December 7, 2024, please call our dedicated assistance line available at 855-278-0557, Monday through Friday, 9:00 AM to 9:00 PM Eastern Time.

67. At GPRMC's suggestion, Plaintiff are desperately trying to mitigate the damages GPRMC caused them.

68. GPRMC also admitted it had inadequate data security prior to the Breach by stating:³¹

We want to assure our community that we are taking this matter very seriously. To help prevent something like this from happening in the future, we have and will continue to take steps to enhance the security of our systems.

69. GPRMC should have had these additional security measures in place before the Breach.

³⁰ <https://gprmc-ok.com/notice-of-security-incident/>

³¹ *Id.*

70. Given the kind of Private Information GPRMC made accessible to hackers, however, Plaintiff are certain to incur additional damages. Because identity thieves have their Private Information, Plaintiff and Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.³²

71. None of this should have happened because the Data Breach was entirely preventable.

D. GPRMC was Aware of the Risk of Cyberattacks.

72. According to the Center for Internet Security, “the health industry experiences more data breaches than any other sector.”³³ This is because “Personal Health Information (PHI) is more valuable on the black market than credit card credentials or regular Personally Identifiable Information (PII). Therefore, there is a higher incentive for cybercriminals to target medical databases. They can sell the PHI and/or use it for their own personal gain.”³⁴

73. “In 2023, more than 540 organizations and 112 million individuals were implicated in healthcare data breaches reported to the HHS Office for Civil Rights (OCR), compared to 590 organizations and 48.6 million impacted individuals in 2022.”³⁵

74. “The number of cybersecurity attacks disrupting the healthcare sector has continued

³² *What happens if I change my Social Security number?*, LEXINGTON LAW (Aug. 10, 2022), <https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html>.

³³ *Data Breaches: In the Healthcare Sector*, CENTER FOR INTERNET SECURITY, <https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector> (last visited April 11, 2024).

³⁴ *Id.*

³⁵ *This Year's Largest Healthcare Data Breaches*, HEALTH IT SECURITY (Dec. 26, 2023), <https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches>.

to be a growing concern. In the last three years, more than 90% of all healthcare organizations have reported at least one security breach which can manifest in denial of service, malicious code, ransomed data, and more.”³⁶

75. “Healthcare organi[z]ations are rich targets for cybercriminals because they hold a large amount of sensitive patient data. This data can be used to commit identity theft or fraud or sold on the black market. Hackers can access this data in many ways, including phishing emails, malware, and unsecured networks.”³⁷

76. It is no secret that “[h]ealthcare data breaches are reaching record highs. Indeed, healthcare now sees more cyberattacks than any other industry. Fully one-third of all cyberattacks are aimed at healthcare institutions. Why? Because healthcare is a valuable and vulnerable target. Hospitals and healthcare institutions are a prime target for cybercrime due to the vast amount of sensitive data they hold.”³⁸

77. The health industry is frequently recognized as one of the most vulnerable industries for a cyberattack.³⁹

³⁶ *6 Industries Most Vulnerable to Cyber Attacks*, WGU (Aug. 3, 2021), <https://www.wgu.edu/blog/6-industries-most-vulnerable-cyber-attacks2108.html>.

³⁷ Troy Beamer, *What Industries Are Most Vulnerable to Cyber Attacks In 2024?*, TECHNEWS (Feb. 27, 2024), <https://www.techbusinessnews.com.au/what-industries-are-most-vulnerable-to-cyberattacks-in-2022/>.

³⁸ *What Industries Are Most Vulnerable to Cyberattacks?*, PSM, <https://www.psmpartners.com/blog/most-targeted-industries-for-cyber-attacks/> (last accessed April 11, 2024).

³⁹ See, e.g., *id.*; Liudmyla Pryimenko, *The 7 Industries Most Vulnerable to Cyberattacks*, EKRAN (Mar. 25, 2024), <https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches>; Ani Petrosyan, *Distribution of cyberattacks across worldwide industries in 2023*, STATISTA (Mar. 22, 2024), <https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/>; *6 Industries Most Vulnerable to Cyber Attacks*, WGU (Aug. 3, 2021), <https://www.wgu.edu/blog/6-industries-most-vulnerable-cyber-attacks2108.html>.

78. GPRMC should have been aware, and indeed was aware, that it was at risk of a data breach that could expose the Private Information that it solicited, collected, stored, and maintained, especially given the rise of healthcare data breaches.

79. GPRMC's assurances to patients that it maintains high standards of cybersecurity are further evidence that GPRMC recognized it had a duty to use reasonable measures to protect the Private Information that it solicited, collected, and maintained.

80. GPRMC was aware of the risks and harm that could result from inadequate data security.

E. GPRMC Could Have Prevented the Data Breach.

81. Data breaches are preventable.⁴⁰ "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."⁴¹ "Organizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"⁴²

82. Most reported data breaches "are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."⁴³

83. Here, many failures laid the groundwork for the Data Breach.

⁴⁰ Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at <https://lawcat.berkeley.edu/record/394088>.

⁴¹ *Id.* at 17.

⁴² *Id.* at 28.

⁴³ *Id.*

84. The FTC has published guidelines that establish reasonable data security practices for businesses.⁴⁴

85. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.⁴⁵

86. The FTC guidelines establish that businesses should protect the confidential 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 for installing vendor-approved patches to correct security problems.⁴⁶

87. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.⁴⁷

88. According to information and belief, GPRMC failed to follow reasonable and necessary industry standards to prevent a data breach, including the FTC's guidelines.

89. Based on allowing its security certificates to lapse and upon information and belief, GPRMC also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's

⁴⁴ *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

Critical Security Controls (CIS CSC), which are well respected authorities in cybersecurity readiness.

90. 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.”⁴⁸

91. To prevent and detect the attack here, GPRMC could and should have taken, as recommended by the Federal Bureau of Investigation, the following measures:

- Implemented 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.
- Enabled 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.
- Scanned all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configured firewalls to block access to known malicious IP addresses.
- Patched 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.

⁴⁸ 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>.

- Managed 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.
- Configured 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.
- Disabled 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.
- Implemented 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.
- Considered disabling Remote Desktop protocol (RDP) if it is not being used.
- Used application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Executed operating system environments or specific programs in a virtualized environment.

- Categorized data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁴⁹

92. According to information and belief, GPRMC failed to do any of the above.

93. To prevent and detect ransomware attacks, GPRMC could and should have recommended its employees, as recommended by the United States Cybersecurity & Infrastructure Security Agency, take the following measures:

- **Updated and patched 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.
- **Used 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).
- **Opened 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.

⁴⁹ *Id.* at 3–4.

- **Kept your personal information safe.** Check a website’s security to ensure the information you submit is encrypted before you provide it.
- **Verified email senders.** If you are unsure whether or not an email is legitimate, try to verify the email’s legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Used and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.⁵⁰

94. In addition, to prevent and detect the Data Breach, including the Breach that resulted in the Data Breach, GPRMC could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Harden internet-facing assets**

⁵⁰ See *Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (revised Sept. 2, 2021), <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (internal citations omitted).

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audits
- **Thoroughly investigate and remediate alerts.**
 - Prioritize and treat commodity malware infections as potential full compromise of the system
- **Include IT professionals in security discussions.**
 - Ensure collaboration among security operations, security administrators, and information technology administrators to configure servers and other endpoints securely
- **Build and maintain credential hygiene**
 - Use multifactor authentication or network level authentication and enforce strong, randomized, just-in-time local administrator passwords
- **Apply principle of least-privilege**
 - Monitor for adversarial activities
 - Hunt for brute force attempts
 - Monitor for cleanup of Event Logs
 - Analyze logon events
- **Harden infrastructure**
 - Utilize 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 Applications⁵¹

95. Given that GPRMC was storing the Private Information of thousands of individuals, GPRMC could and should have implemented all of the above measures to prevent and detect cyberattacks.

96. Specifically, among other failures, GPRMC had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.⁵²

97. Moreover, it is well-established industry standard practice for a business to dispose of confidential Private Information once it is no longer needed.⁵³

98. The FTC has repeatedly emphasized the importance of disposing of unnecessary Private Information: “Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it’s not on your system, it can’t be stolen by hackers.”⁵⁴ Rather than following this basic standard of care, GPRMC kept millions of individuals’ unencrypted Private Information on their inadequately secured systems indefinitely.

⁵¹ See *Human-operated ransomware attacks: A preventable disaster*, MICROSOFT THREAT INTELLIGENCE (Mar 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

⁵² See Adnan Raja, *How to Safeguard Your Business Data With Encryption*, DATAINSIDER (Aug. 14, 2018), <https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption>.

⁵³ See *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>.

⁵⁴ *Id.* at 6.

99. In sum, the Data Breach could have been easily prevented through standard practices like the use of industry standard network segmentation and encryption of all Private Information—which GPRMC negligently failed to do.

100. Further, the scope of the Data Breach could have been dramatically reduced had GPRMC utilized proper record retention and destruction practices—but GPRMC negligently did no such thing.

F. GPRMC had an Obligation to Protect Private Information Under the Law and the Applicable Standard of Care.

101. As a healthcare service provider handling medical patient data and providing services to hospitals and healthcare organizations, GPRMC is a covered entity under HIPAA (45 C.F.R. § 160.103). As such, GPRMC is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C (“Security Standards for the Protection of Electronic Protected Health Information”).

102. HIPAA’s Privacy Rule establishes national standards for protecting health information, including health information that is kept or transferred in electronic form.

103. GPRMC is required to “comply with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302.

104. “Electronic protected health information” is “individually identifiable health information . . . that is: (i) transmitted by electronic media; [or] (ii) maintained in electronic media[.]” 45 C.F.R. § 160.103.

105. The HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C, requires GPRMC to:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information it or any business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information; and
- d. Ensure compliance by its workforce.

106. HIPAA also requires GPRMC to “review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information[.]” 45 C.F.R. § 164.306(e).

107. Additionally, HIPAA requires GPRMC to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights[.]” 45 C.F.R. § 164.312(a)(1).

108. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, further requires GPRMC to provide notice of the Data Breach to each affected individual “without unreasonable delay and in no case later than 60 days following discovery of [the] breach[.]”

109. GPRMC was also prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 (the “FTC Act”), from engaging in “unfair or deceptive acts or practices in or affecting commerce[.]” The FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in

violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

110. GPRMC is further required by various states' laws and regulations to protect Plaintiff's and Class Members' Private Information.

111. GPRMC owed a duty to Plaintiff and the Class to design, maintain, and test its computer and email systems to ensure that the Private Information in its possession and control was adequately secured and protected.

112. GPRMC owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees (and any others who accessed Private Information within its computer systems) on how to adequately protect Private Information.

113. GPRMC owed a duty to Plaintiff and the Class to implement processes that would detect a breach of its data security systems in a timely manner.

114. GPRMC owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

115. GPRMC owed a duty to Plaintiff and the Class to adequately train and supervise its employees to identify and avoid any phishing emails that make it past its email filtering service.

116. GPRMC owed a duty to Plaintiff and the Class to disclose if their computer systems and data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in individuals' decisions to entrust GPRMC with their Private Information.

117. GPRMC owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

118. GPRMC owed a duty of care to Plaintiff and the Class because they were foreseeable and probable victims of any inadequate data security practices.

G. Plaintiff's Individual Experience

119. Plaintiff Evans entrusted his Private Information to GPRMC with the reasonable expectation and mutual understanding that GPRMC would keep his Private Information secure from unauthorized access.

120. By soliciting and accepting Plaintiff Evans' Private Information, GPRMC agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

121. GPRMC was in possession of Plaintiff Evans's Private Information before, during, and after the Data Breach.

122. After the Data Breach, Plaintiff Evans received a Notice Letter from GPRMC, notifying him that an unauthorized party gained access to GPRMC's network between September 5th through the 8th, 2024, and was potentially accessed without authorization.⁵⁵

123. Following the Data Breach, Plaintiff Evans made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports. In total, Plaintiff Evans estimates he has already spent hours responding to the Data Breach. Plaintiff Evans has also experienced an increased amount of spam that he now needs to monitor closely.

124. Plaintiff Evans will be forced to expend additional time to review his credit reports and monitor his accounts for the rest of his life. This is time, spent at Defendant's direction, which has been lost forever and cannot be recaptured.

⁵⁵ Ex. 1.

125. Plaintiff Evans places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Evans entrusted GPRMC with his Private Information with the understanding that GPRMC would keep his information secure and would employ reasonable and adequate data security measures to ensure that his Private Information would not be compromised.

126. Plaintiff Evans has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

127. As a direct and traceable result of the Data Breach, Plaintiff Evans suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of his bargain because GPRMC did not adequately protect his Private Information; (d) emotional distress because identity thieves now possess his first and last name paired with his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and published on the dark web; (f) diminution in the value of his Private Information, a form of intangible property that GPRMC obtained from Plaintiff Evans and/or his medical providers; and (g) other economic and non-economic harm.

128. Plaintiff Evans has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information

stolen in the Data Breach.⁵⁶

129. Plaintiff Evans has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches. Absent Court intervention, Plaintiff Evans' Private Information will be wholly unprotected and at-risk of future data breaches.

V. CLASS ACTION ALLEGATIONS

130. Plaintiff incorporate by reference all preceding factual paragraphs as if fully restated here.

131. Plaintiff bring this action against GPRMC on behalf of themselves and all other individuals similarly situated under 12 O.S. § 2023. Plaintiff assert all claims on behalf of a nationwide class (the "Class") defined as follows:

All persons who were impacted by the Data Breach discovered publicly announced by Defendant in November 2024 (the "Class").

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

133. Plaintiff reserves the right to amend or modify the above Class definition or to propose subclasses in subsequent pleadings and motions for class certification.

⁵⁶ *Id.*

134. Plaintiff anticipates the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

135. The proposed Class meets the requirements of 12 O.S. § 2023.

136. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. The total number of individuals affected is at least 133,149.

137. **Typicality:** Plaintiff's claims are typical of the claims of the Class because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff and all members of the Class were injured by the same wrongful acts, practices, and omissions committed by GPRMC, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that gives rise to the claims of all Class Members.

138. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class. Plaintiff has retained counsel competent and highly experienced in data breach class action litigation, and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

139. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for individual members of the Class to effectively redress GPRMC's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a

potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

140. **Commonality and Predominance:** Defendant engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' Private Information was stored on the same network and unlawfully accessed in the same way. There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

- a. Whether Defendant engaged in the wrongful conduct alleged herein;
- b. Whether Defendant owed a duty to Plaintiff and Class Members to adequately protect their Private Information;
- c. Whether Defendant breached its duty to Plaintiff and Class Members to adequately protect their Private Information;
- d. 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;
- e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- f. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

- g. Whether Defendant knew or should have known that its computer and network security systems, or the computer and network security systems of its vendors, were vulnerable to cyberattacks;
- h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;
- i. Whether Defendant was negligent in permitting unencrypted Private Information belonging to millions of individuals to be stored within its network;
- j. Whether Defendant was negligent in failing to adhere to reasonable data retention policies;
- k. Whether Defendant breached implied contractual duties to Plaintiff and the Class to use reasonable care in protecting their Private Information;
- l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiff and Class Members;
- m. Whether Defendant should have discovered the Data Breach sooner;
- n. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;
- o. Whether Defendant continues to breach duties owed to Plaintiff and the Class;
- p. Whether Plaintiff and the Class suffered injuries as a proximate result of Defendant's negligent actions or failures to act;
- q. Whether Defendant was negligent in selecting, supervising, and/or monitoring vendors;

- r. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and
- s. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

141. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class wide basis.

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

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION NEGLIGENCE

(On Behalf of Plaintiff and the Class)

143. Plaintiff re-alleges and incorporates by reference all preceding factual paragraphs as though fully set forth herein.

144. GPRMC solicited, collected, stored, and maintained the Private Information of Plaintiff and Class Members on inadequately secured computer systems and networks.

145. Upon accepting and storing Plaintiff's and Class Members' Private Information on its computer systems and networks, Defendant undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information from unauthorized access and disclosure.

146. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure

that its computer systems and networks, and the personnel responsible for them, adequately protected the Private Information.

147. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

148. Defendant had full knowledge of the sensitivity of the Private Information in its possession and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully accessed or disclosed. Plaintiff and Class Members were therefore the foreseeable victims of any inadequate data security practices.

149. Defendant's duty to implement and maintain reasonable data security practices arose as a result of the special relationship that exists between Defendant and consumers, which is recognized by laws and regulations, including, but not limited to, HIPAA, the FTC Act, and common law.

150. Defendant was in a superior position to ensure its data security practices were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

151. Defendant knew Plaintiff and Class Members relied on it to protect their Private Information. Plaintiff and Class Members were not in a position to assess the data security practices used by Defendant. Because they had no means to identify Defendant's security deficiencies, Plaintiff and Class Members had no opportunity to safeguard their Private Information from cybercriminals. Defendant exercised control over the Private Information stored on its systems and networks; accordingly, Defendant was best positioned and most capable of preventing the harms caused by the Data Breach.

152. Defendant was aware, or should have been aware, of the fact that cybercriminals routinely target healthcare entities through cyberattacks in an attempt to steal valuable Private Information. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

153. Defendant owed Plaintiff and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiff and Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

154. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to such risk, or defeats protections put in place to guard against that risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

155. Defendant had a duty to protect and safeguard the Private Information of Plaintiff and the Class from unauthorized access and disclosure. Additionally, Defendant owed Plaintiff and the Class a duty:

- a. to exercise reasonable care in designing, implementing, maintaining, monitoring, and testing its networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' Private Information was adequately secured from impermissible release, disclosure, and publication;

- b. to protect Plaintiff's and Class Members' Private Information by using reasonable and adequate data security practices and procedures;
- c. to implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and
- d. to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

156. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information.

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

- a. Failing to adopt, implement, and maintain adequate data security measures to safeguard Plaintiff's and Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failing to ensure its email systems had plans in place to maintain reasonable data security safeguards;
- d. Failing to implement and maintain adequate mitigation policies and procedures;
- e. Allowing unauthorized access to Plaintiff's and Class Members' Private Information;
- f. Failing to detect in a timely manner that Plaintiff's and Class Members' Private Information had been compromised; and

- g. Failing to timely notify Plaintiff and Class Members about the Data Breach so they could take appropriate steps to mitigate the potential for identity theft and other damages.

158. Defendant's willful failure to abide by its duties to Plaintiff and Class Members was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

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

160. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

161. As a direct and proximate result of Defendant's negligent conduct, including, but not limited to, its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

162. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class Members while it was within Defendant's possession and control.

163. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their Private Information and mitigate the impact of the Data Breach.

164. Plaintiff and Class Members could have taken actions earlier had they been timely notified of the Data Breach.

165. Plaintiff and Class Members could have enrolled in credit monitoring, instituted credit freezes, and changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

166. Plaintiff and Class Members suffered harm from Defendant's delay in notifying them of the Data Breach.

167. As a direct and proximate result of Defendant's conduct, including, but not limited to, Defendant's failure to implement and maintain reasonable data security practices and procedures, Plaintiff and Class Members have suffered or will suffer injury and damages, including, but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost time and opportunity costs associated with efforts expended to address and 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 fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) 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 its continued possession; and (viii) future costs in terms of time, effort, and money

that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

168. The damages Plaintiff and the Class have suffered and will suffer (as alleged above) were and are the direct and proximate result of Defendant's negligent conduct.

169. Plaintiff and the Class have suffered cognizable injuries and are entitled to actual and punitive damages in an amount to be proven at trial.

**SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)**

170. Plaintiff re-alleges and incorporates all preceding factual paragraphs as though fully set forth herein.

171. Defendant had a duty to implement and maintain reasonable data security practices pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect sensitive and confidential data.

172. 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 PII/PHI. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

173. Defendant solicited, collected, stored, and maintained Plaintiff's and Class Members' Private Information as part of its regular business, which affects commerce.

174. Defendant violated the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and by failing to comply with applicable industry standards, as described herein.

175. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to implement and maintain fair, reasonable, and adequate data security practices to safeguard Plaintiff's and Class Members' Private Information, and by failing to provide prompt notice of the Data Breach without unreasonable delay.

176. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

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

178. 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, like GPRMC, that fail to employ reasonable data security measures and avoid unfair and deceptive practices, causing the same harm as that suffered by Plaintiff and the Class.

179. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

180. Defendant's violations of the FTC Act constitute negligence *per se*.

181. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

182. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

183. Defendant also had a duty to use reasonable security measures under HIPAA, which requires covered entities, like GPRMC, to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this action constitutes "protected health information" within the meaning of HIPAA.

184. 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 Private Information. HHS subsequently promulgated multiple regulations under the authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.304, 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).

185. Defendant's violations of HIPAA constitute negligence *per se*.

186. Plaintiff and the Class are within the class of persons HIPAA was intended to protect.

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

188. Defendant's duty to use reasonable care in protecting Plaintiff's and Class Members' Private Information arose not only as a result of the statutes and regulations described

above, but also because Defendant is bound by industry standards to protect and secure Private Information in its possession and control.

189. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual instances of identity theft or fraud; (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, fraud, and/or unauthorized use of their Private Information; (iv) lost time and opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach, including, but not limited to, time and resources spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) costs associated with placing or removing freezes on credit reports; (vi) 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 its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the ongoing impact of the Data Breach for the remainder of the lives of Plaintiff and the Class.

190. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer imminent and impending injuries arising from the increased risk of future fraud and identity theft.

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

192. Plaintiff and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

**THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)**

193. Plaintiff re-alleges and incorporates all preceding factual paragraphs as though fully set forth herein.

194. Defendant solicited, collected, stored, and maintained Plaintiff's and Class Members' Private Information, including their Social Security numbers and other sensitive personal and medical information, as part of Defendant's regular business practices.

195. Plaintiff and Class Members were required to provide their Private Information to Defendant in order to receive medical services. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for medical services.

196. Defendant solicited and accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing medical services to Plaintiff and Class Members.

197. In delivering, directly or indirectly, their Private Information to Defendant and paying for healthcare services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard their Private Information.

198. Plaintiff and Class Members reasonably expected that the Private Information they entrusted to GPRMC, in order to receive medical services would remain confidential and would not be shared or disclosed to criminal third parties.

199. Plaintiff and Defendant had a mutual understanding that GPRMC would implement and maintain adequate and reasonable data security practices and procedures to protect Plaintiff's and Class Members' sensitive Private Information. Plaintiff and Defendant also shared an

expectation and understanding that GPRMC would not share or disclose, whether intentionally or unintentionally, the sensitive Private Information in its possession and control.

200. Based on Defendant's representations, legal obligations, and acceptance of Plaintiff's and Class Members' Private Information, Defendant had a duty to safeguard the Private Information in its possession through the use of reasonable data security practices.

201. When Plaintiff and Class Members paid money and provided their Private Information to GPRMC and/or their healthcare providers, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with Defendant.

202. Defendant entered into implied contracts with Plaintiff and the Class under which Defendant agreed to comply with its statutory and common law duties to safeguard and protect Plaintiff's and Class Members' Private Information and to timely notify Plaintiff and Class Members of a data breach.

203. The implied promise of confidentiality includes consideration beyond those pre-existing duties owed under Section 5 of the FTC Act, HIPAA, and other state and federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

204. The implied promises include, but are not limited to: (i) taking steps to ensure any agents or vendors who are granted access to Private Information protect the confidentiality of that information; (ii) taking steps to ensure that Private Information in the possession and control of Defendant, its agents, and/or vendors is restricted and limited to achieve an authorized medical purpose; (iii) restricting access to qualified and trained agents and/or vendors; (iv) designing and implementing appropriate retention policies to protect the Private Information from unauthorized access and disclosure; (v) applying or requiring proper encryption of the Private Information; (vi)

requiring multifactor authentication for access to the Private Information; and (vii) other steps necessary to protect against foreseeable data breaches.

205. Plaintiff and Class Members (or their doctors and healthcare providers) would not have entrusted their Private Information to Defendant in the absence of such implied contracts.

206. Defendant recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance to Plaintiff and Class Members.

207. Had Defendant disclosed to Plaintiff and Class Members (or their doctors and healthcare providers) that it did not have adequate data security practices to secure their Private Information, Plaintiff and Class Members (or their doctors and healthcare providers) would not have provided their Private Information to Defendant.

208. Plaintiff and Class Members (or their doctors and healthcare providers) fully performed their obligations under the implied contracts with Defendant.

209. Defendant breached the implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

210. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it solicited and collected Plaintiff's and Class Members' Private Information.

211. Alternatively, Plaintiff and Class Members were the intended beneficiaries of data protection agreements entered into between Defendant and healthcare providers.

212. Plaintiff and the Class have suffered injuries as described herein, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

**FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)**

213. Plaintiff re-alleges and incorporates all preceding factual paragraphs as though fully set forth herein.

214. Plaintiff alleges this claim in the alternative to his breach of implied contract claim.

215. Plaintiff and the Class provided their Private Information to GPRMC in order to receive medical services.

216. By conferring their Private Information to Defendant, Plaintiff and Class Members reasonably understood Defendant would be responsible for securing their Private Information from unauthorized access and disclosure.

217. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including from money it makes based on protecting Plaintiff's and Class Members' Private Information.

218. Plaintiff and Class Members paid Defendant and/or their healthcare providers a certain sum of money, which was used to fund data security via contracts with Defendant.

219. As such, a portion of the payments made by or on behalf of Plaintiff and the Class was to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

220. There is a direct nexus between money paid to Defendant and the requirement that Defendant keep Plaintiff's and Class Members' Private Information confidential and protected

from unauthorized access and disclosure.

221. Protecting the Private Information of Plaintiff and Class Members is integral to Defendant's business. Without their Private Information, Defendant would be unable to provide services comprising Defendant's core business.

222. Plaintiff's and Class Members' Private Information has monetary value.

223. Plaintiff and Class Members directly and indirectly conferred a monetary benefit on Defendant. They indirectly conferred a monetary benefit on Defendant by purchasing goods and/or services from entities that contracted with Defendant, and from which Defendant received compensation to protect certain data. Plaintiff and Class Members directly conferred a monetary benefit on Defendant by supplying their Private Information, from which Defendant derives its business, and which should have been protected with adequate data security.

224. Defendant solicited, collected, stored, and maintained Plaintiff's and Class Members' Private Information, and as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff and the Class. Defendant profited from these transactions and used Plaintiff's and Class Members' Private Information for business purposes.

225. Indeed, Plaintiff and Class Members who were patients of GPRMC provided monetary payment to GPRMC and therefore conferred a benefit unto GPRMC.

226. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

227. Under the facts and circumstances outlined above, however, it is inequitable for Defendant to retain that benefit without payment of the value thereof.

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

229. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits 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 decision to prioritize its own profits over the requisite data security.

230. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures.

231. Defendant acquired Plaintiff's and Class Members' Private Information through inequitable means in that it failed to disclose its inadequate data security practices, as previously alleged.

232. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have allowed Defendant to collect their Private Information.

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

234. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including, but not limited to: (i) actual identity theft and fraud; (ii) loss of the opportunity to control 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, fraud, and/or unauthorized use of their Private Information; (v) lost time and opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach, including, but not limited to, effort and time spent researching how to prevent, detect, contest, and recover from identity theft; (vi) 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; and/or (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

235. 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.

236. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, all gains that they unjustly received.

FIFTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

237. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

238. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information that Plaintiff and Class Members entrusted to Defendant.

239. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

240. Plaintiff and the Class entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

241. Plaintiff and the Class also entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

242. Defendant voluntarily received Plaintiff's and Class Members' Private Information in confidence with the understanding that their Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

243. As a result of Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

244. As a direct and proximate cause of Defendant's actions and omissions, Plaintiff and the Class have suffered damages.

245. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information as well as the resulting damages.

246. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendant knew or should have known its methods of accepting and securing

Plaintiff's and Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' Private Information.

247. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) 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, 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 actual present and future 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 current and former people; and (viii) present and 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.

248. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class Members 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.

SIXTH CAUSE OF ACTION
OKLAHOMA CONSUMER PROTECTION ACT
Okla. Stat. Tit. 15 §§ 751, et seq
(On Behalf of Plaintiff and the Class)

249. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

250. Defendant is a “person,” as meant by Okla. Stat. tit. 15, § 752(1).

251. Defendant’s advertising, offering, and provision of health care services to Plaintiff and Class Members constitute “consumer transactions” under Okla. Stat. tit. 15, § 752(2).

252. Defendant in the course of its business, committed deception and unlawful practices, including but not limited to the following:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff’s and Class Members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff’s and Class Members’ Private Information, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class Members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members’ Private Information;
- f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff and Class Members’ Private Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members’ Private Information.

253. Defendant’s representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant’s data security and ability to protect the confidentiality of patients’ Private Information.

254. Had Defendant disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

255. Defendant was trusted with patients sensitive and valuable Private Information, including Plaintiff and Class Members.

256. Defendant accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

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

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

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

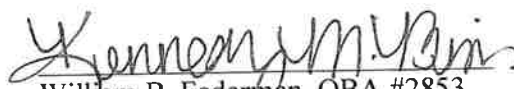
- a. For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and her counsel as Class Counsel;
- b. For an order declaring that Defendant's conduct violates the laws referenced herein;
- c. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- d. For damages in amounts to be determined by the Court and/or jury;
- e. For an award of statutory damages or penalties to the extent available;
- f. For pre-judgment interest on all amounts awarded;
- g. For an order of restitution and all other forms of monetary relief; and
- h. Such other and further relief as the Court deems necessary and appropriate.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on any and all issues raised in this Class Action Petition so triable as of right.

Dated: November 20, 2024

Respectfully submitted,



William B. Federman, OBA #2853

Kennedy M. Brian, OBA #34617

FEDERMAN & SHERWOOD

10205 North Pennsylvania Avenue

Oklahoma City, OK 73120

T: (405) 235-1560

E: wbf@federmanlaw.com

E: kpb@federmanlaw.com

EKSM, LLP

Leigh S. Montgomery*

Texas Bar No. 24052214
lmontgomery@eksm.com
1105 Milford Street
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455

**ATTORNEYS FOR PLAINTIFFS AND THE
PUTATIVE CLASS**
(* denotes *pro hac vice* forthcoming)