IN THE CIRCUIT COURT OF CLAY COUNTY, MISSOURI
7TH JUDICIAL CIRCUIT

BESSIE JACKSON, individually and on behalf of all others similarly situated, Plaintiff, v. BOARD OF TRUSTEES OF NORTH KANSAS CITY HOSPITAL, MERITAS HEALTH CORPORATION, and PERRY JOHNSON & ASSOCIATES, INC., Defendants.	Case No. _____ CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION PETITION

Plaintiff Bessie Jackson ("Plaintiff"), individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, brings this Class Action Petition against Defendants Board of Trustees of North Kansas City Hospital ("NKCH"), Meritas Health Corporation ("Meritas"), and Perry Johnson & Associates, Inc. ("PJA") (collectively, "Defendants"), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard her and approximately 502,438 other individuals' personally identifying information ("PII") and personal health information ("PHI"), including names, Social Security numbers, dates of birth, addresses, medical record numbers, encounter numbers, medical information, and dates/times of service.

2. NKCH are the Board of Trustees for a 451-bed acute care hospital North Kansas City Hospital. Meritas, a wholly-owned subsidiary of NKCH, is a multi-specialty group practice and physician network. PJA is a third-party vendor of health information technology solutions used by NKCH and Meritas.

3. Between approximately March 27, 2023, and May 2, 2023, an unauthorized third party gained access to PJA's network system and obtained files containing information about NKCH's and Meritas's current and former patients (the "Data Breach").

4. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect NKCH's and Meritas's patients' PII/PHI from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons who provided their PII/PHI to NKCH and Meritas and whose PII/PHI was exposed as a result of the Data Breach, which occurred between approximately March 27, 2023, and May 2, 2023.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of express contract, breach of implied contract, unjust enrichment, and violations of the Missouri Merchandising Practices Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Bessie Jackson

7. Plaintiff Bessie Jackson is a citizen of Missouri.

8. Plaintiff obtained healthcare services from NKCH and Meritas. As a condition of receiving services, NKCH and Meritas required Plaintiff to provide them with her PII/PHI.

9. Based on representations made by NKCH and Meritas, Plaintiff believed NKCH and Meritas had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff provided her PII/PHI to NKCH and Meritas in connection with receiving healthcare services provided by NKCH and Meritas.

10. At all relevant times, Defendants stored and maintained Plaintiff's PII/PHI on their network systems.

11. Plaintiff takes great care to protect her PII/PHI. Had Plaintiff known that NKCH and Meritas do not adequately protect the PII/PHI in their possession, including by contracting with companies that do not adequately protect the PII/PHI in their possession, she would not have obtained healthcare services from NKCH and Meritas or agreed to entrust them with her PII/PHI.

12. Plaintiff received a letter from NKCH and Meritas notifying her that her PII/PHI was affected in the Data Breach.

13. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include adequate data security.

Defendant Board of Trustees of North Kansas City Hospital

14. Defendant Board of Trustees of North Kansas City Hospital is a municipal entity of North Kansas City, Missouri established pursuant to Mo. Rev. Stat. §§ 96.150 and 96.160.

Defendant Meritas Health Corporation

15. Defendant Meritas Health Corporation is a Missouri nonprofit corporation with its principal place of business located at 2800 Clay Edwards Dr., North Kansas City, MO 64116. It may be served through its registered agent: Jennifer Kozinn, 2800 Clay Edwards Dr., North Kansas City, MO 64116.

Defendant Perry Johnson & Associates, Inc.

16. Defendant Perry Johnson & Associates is a Nevada corporation with its principal place of business at 1489 W Warm Springs Rd., Henderson, NV 89014. It may be served through its registered agent C T Corporation System, 701 S. Carson St., Suite 200, Carson City, NV 89701.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over Plaintiff's claims pursuant to Mo. Rev. Stat. § 478.070.

18. This Court has personal jurisdiction over Defendant Board of Trustees of North Kansas City Hospital because it is a public entity and does significant business in Missouri.

19. This Court has personal jurisdiction over Defendant Meritas Health Corporation because it is a corporation incorporated under the laws of Missouri, has its principal place of business in Missouri, and does significant business in Missouri.

20. This Court has personal jurisdiction over Defendant Perry Johnson & Associates, Inc. because it transacts business within this state and makes or performs contracts within this state.

21. Venue is proper in this Circuit pursuant to Mo. Rev. Stat. §§ 508.010 and 508.050 because NKCH is situated in Clay County, Meritas's principal place of business is in Clay County, and a substantial part of the events giving rise to Plaintiff's claims arose in Clay County.

FACTUAL ALLEGATIONS

Overview of Defendants

22. NKCH is "an acute care facility with 451 licensed beds and 550 physicians representing 49 medical specialties."[1] "Through [its] Meritas Health subsidiary, NKCH offers the largest network of physician practices in the Northland, with more than 280 primary and specialty care doctors and advanced practice providers."[2]

23. In the regular course of its business, NKCH and Meritas collect and maintain the PII/PHI of their current and former patients. NKCH and Meritas required Plaintiff and Class members to provide their PII/PHI as a condition of receiving healthcare services from NKCH and Meritas.

24. NKCH's website contains a Notice of Privacy Practices (the "Privacy Policy") that applies to NKCH and Meritas.[3] NKCH's website states, "The purpose of this policy is to ensure that, your health information is used and disclosed only: (1) for your treatment, payment of our services or our operations, (2) upon your authorization, or (3) if allowed by state or federal laws."[4]

---

[1] *About Us*, N. KAN. CITY HOSP., https://www.nkch.org/about-us/ (last accessed Jan. 9, 2024).
[2] *Id.*
[3] *Notice of Privacy Practices*, N. KAN. CITY HOSP., https://www.nkch.org/assets/documents/notice-of-pp.pdf (last accessed Jan. 9, 2024) [hereinafter "*Privacy Policy*"].
[4] *Patient Rights & Policies - Notice of Privacy Practices*, N. KAN. CITY HOSP., https://www.nkch.org/patients-and-guests/for-patients/during-your-visit/patient-rights-policies/notice-of-privacy-practices (last accessed Jan. 9, 2024).

25. In the Privacy Policy, NKCH and Meritas admit they are required by the Health Insurance Portability and Accountability Act ("HIPAA") to "maintain the privacy of patients' health information."[5]

26. NKCH and Meritas promise their "privacy policies and practices protect confidential health information that identifies you or could be used to identify you."[6] They further promise patients' "PHI will not be used or disclosed without written authorization from you, except as described in this notice or as otherwise permitted by federal and state health information privacy laws."[7]

27. The Privacy Policy lists the ways NKCH and Meritas can use patients' information, including for treatment, payment, healthcare operations, and fundraising.[8]

28. The Privacy Policy promises patients they will be notified in the event of a data breach.[9] It states, "We will keep your medical information private and secure as required by law. If any of your medical information is breached as described in HIPAA, we will notify you without unreasonable delay but within 60 days following the discovery of a breach."[10]

29. The Privacy Policy states "uses and disclosures of PHI for marketing purposes or sales of your PHI require your written authorization."[11] NKCH and Meritas go on to state, "Other uses and disclosures of health information not covered by this notice or by the laws that apply to us will be made only with your written authorization."[12]

---

[5] *Privacy Policy, supra* note 3.
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*

30. PJA "provides medical transcription services to various healthcare organizations."[13] NKCH and Meritas used PJA for medical transcription services.[14]

31. Plaintiff and Class members are current or former patients of NKCH and Meritas and entrusted NKCH and Meritas with their PII/PHI.

The Data Breach

32. Between approximately March 27, 2023, and May 2, 2023, "An unauthorized party gained access to the PJ&A network . . . and, during that time, acquired copies of certain files from PJ&A systems."[15]

33. According to the Notice of Data Security Incident posted on PJA's website, the PII/PHI affected in the Data Breach included names, dates of birth, addresses, medical record numbers, hospital account numbers, admission diagnoses, dates and times of service, Social Security numbers, insurance information, clinical information such as laboratory and diagnostic testing results, medications, treatment facility names, and healthcare provider names.[16]

34. NKCH's Privacy Policy promises its patients that, "If any of your medical information is breached as described in HIPAA, we will notify you without unreasonable delay but within 60 days following the discovery of a breach."[17] PJA informed NKCH of the Data Breach

[13] *Cyber Incident Notice*, PERRY JOHNSON & ASSOCS., https://www.pjats.com/downloads/Notice.pdf (last accessed Jan. 9, 2024) [hereinafter "*PJA Notice*"].
[14] *PJA Data Event*, N. KAN. CITY HOSP. (Jan. 3, 2024), https://www.nkch.org/pja-data-event/ (last accessed Jan. 9, 2024).
[15] *PJA Notice*, *supra* note 13.
[16] *Id.*
[17] *Privacy Policy*, *supra* note 3.

on July 21, 2023,[18] but NKCH failed to notify its patients that their information was compromised in the Data Breach until approximately January 3, 2024, over five months later.[19]

35. NKCH's and Meritas's failure to promptly notify Plaintiff and Class members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

Defendants Knew that Criminals Target PII/PHI

36. At all relevant times, Defendants knew, or should have known, that the information they collected was a target for malicious actors. Indeed, NKCH's Privacy Policy explicitly promises patients will be notified if a data breach occurs.[20] Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that Defendants should have anticipated and guarded against.

37. It is well known among companies that store sensitive personally identifying information that such information—such as the PII/PHI stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata

[18] *PJA Data Event*, *supra* note 14.
[19] *See id.*
[20] *See Privacy Policy*, *supra* note 3.

breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[21]

38. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient records exposed.[22] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[23]

39. PII/PHI is a valuable property right.[24] The value of PII/PHI as a commodity is measurable.[25] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[26] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[27] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

---

[21] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[22] *See 2023 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last accessed Jan. 9, 2024).

[23] *See id*.

[24] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[25] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[26] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[27] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

40. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

41. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[28] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[29]

42. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[30] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[31]

---

[28] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[29] *Id.*

[30] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[31] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

43. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[32] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[33]

44. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[34]

45. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

[32] Steager, *supra* note 28.
[33] *Id.*
[34] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

46. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[35] [36]

47. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[37]

48. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[38]

49. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records

---

[35] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Jan. 9, 2024).

[36] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[37] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[38] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed Jan. 9, 2024).

that can plague victims' medical and financial lives for years."[39] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[40] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [41] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[42]

50. Theft of SSNs also creates a particularly alarming situation for victims because SSNs cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse of her SSN. Thus, a new SSN will not be provided until after the harm has already been suffered by the victim.

51. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[43]

---

[39] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[40] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 31.
[41] *See What to Know About Medical Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Jan. 9, 2024).
[42] *Id.*
[43] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

52. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services neither sought nor received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own. [44]

53. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately

[44] *See* Dixon & Emerson, *supra* note 39.

three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[45]

Damages Sustained by Plaintiff and Class Members

54. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

CLASS ALLEGATIONS

55. This action is brought and may be properly maintained as a class action pursuant to Mo. Sup. Ct. R. 52.08.

56. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

> All United States residents who gave their PII/PHI to NKCH or Meritas whose PII/PHI was compromised in the Data Breach by unauthorized persons, including all United States residents who were sent a notice of the Data Breach.

57. Excluded from the Class are Board of Trustees of North Kansas City Hospital, and its affiliates, parents, subsidiaries, employees, officers, agents, and directors; Meritas Health

[45] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

Corporation, and its affiliates, parents, subsidiaries, employees, officers, agents, and directors; and Perry Johnson & Associates, Inc., and its affiliates, parents, subsidiaries, employees, officers, agents, and directors; as well as the judge(s) presiding over this matter and the clerks of said judge.

58. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

59. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. NKCH disclosed to the Department of Health and Human Services that approximately 502,438 individuals were affected by the Data Breach.[46]

60. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendants had duties not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d. Whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

e. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiff and Class members;

[46] *Cases Currently Under Investigation*, DEP'T HEALTH & HUM. SERVS., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Jan. 9, 2024).

f. Whether Defendants breached their duties to protect Plaintiff's and Class members' PII/PHI; and

g. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

61. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

62. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

63. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

64. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members

could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
Against PJA and Meritas Health Only

65. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

66. Plaintiff brings this claim individually and on behalf of all Class members against PJA and Meritas only.

67. PJA and Meritas owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in their possession, custody, or control.

68. PJA and Meritas knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. PJA and Meritas knew or should have known of the many data breaches that targeted healthcare provides that collect and store PII/PHI in recent years.

69. Given the nature of PJA's and Meritas's businesses, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, PJA and Meritas should have identified the vulnerabilities to their systems and their third-party vendor's systems and prevented the Data Breach from occurring.

70. PJA and Meritas breached these duties by failing, or contracting with companies that failed to, to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to them—including Plaintiff's and Class members' PII/PHI.

71. It was reasonably foreseeable to PJA and Meritas that their failure to, or contracting with companies that failed to, exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

72. But for PJA's and Meritas's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

73. As a result of PJA's and Meritas's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact

of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE
Against PJA and Meritas Only

74. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

75. Plaintiff brings this claim individually and on behalf of all Class members against PJA and Meritas only.

76. PJA's and Meritas's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

77. PJA's and Meritas's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as PJA and Meritas, of failing to employ reasonable measures to protect and secure PII/PHI.

78. PJA and Meritas violated the HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and other Class members' PII/PHI, by failing to provide timely notice, and by not complying with applicable industry standards. PJA's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving

PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

79. PJA's and Meritas's violations of the HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

80. Plaintiff and Class members are within the class of persons that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

81. The harm occurring as a result of the Data Breach is the type of harm that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class members as a result of the Data Brach.

82. It was reasonably foreseeable to PJA and Meritas that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

83. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of PJA's and Meritas's violations of the HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated

with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY
Against Meritas Only

84. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

85. This claim is brought by Plaintiff on behalf of all Class members who provided their PII/PHI to Meritas against Meritas only.

86. Plaintiff and Class members gave Meritas their PII/PHI in confidence, believing that Meritas would protect that information. Plaintiff and Class members would not have provided Meritas with this information had they known it would not be adequately protected. Meritas's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between Meritas and Plaintiff and Class members. In light of this relationship, Meritas must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

87. Due to the nature of the relationship between Meritas and Plaintiff and Class members, Plaintiff and Class members were entirely reliant upon Meritas to ensure that their PII/PHI was adequately protected. Plaintiff and Class members had no way of verifying or

influencing the nature and extent of Meritas's or its third-party vendor's data security policies and practices, and Meritas was in an exclusive position to guard against the Data Breach.

88. Meritas has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by contracting with companies that failed to properly protect the integrity of the system containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that its collected and shared.

89. As a direct and proximate result of Meritas's breaches of their fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF EXPRESS CONTRACT
Against NKCH and Meritas Only

90. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

91. This claim is brought by Plaintiff on behalf of all Class members who provided their PII/PHI to NKCH and Meritas against NKCH and Meritas only.

92. Plaintiff and Class members and NKCH and Meritas entered into written agreements regarding the services that NKCH and Meritas was to provide to Plaintiff and Class members. Plaintiff and Class members paid NKCH and Meritas monies, directly or through an insurance carrier and provided NKCH and Meritas with their PII/PHI as consideration for these agreements. NKCH and Meritas's document entitled "Notice of Privacy Practices" is evidence that data security was a material term of these contracts.

93. Plaintiff and Class members complied with the express contract when they paid NKCH and Meritas and provided their PII/PHI to NKCH and Meritas.

94. NKCH and Meritas breached its obligations under the contracts between themselves and Plaintiff and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI.

95. Plaintiff and all other Class members were damaged by NKCH's and Meritas's breach of express contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

COUNT V
BREACH OF IMPLIED CONTRACT
Against NKCH and Meritas Only

96. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

97. This claim is brought by Plaintiff on behalf of all Class members who provided their PII/PHI to NKCH and Meritas against NKCH and Meritas only.

98. In connection with receiving healthcare services, Plaintiff and all other Class members entered into implied contracts with NKCH and Meritas.

99. Pursuant to these implied contracts, Plaintiff and Class members paid money to NKCH and Meritas, directly or through their insurance, and provided NKCH and Meritas with their PII/PHI. In exchange, NKCH and Meritas agreed to, among other things, and Plaintiff and Class members understood that NKCH and Meritas would: (1) provide services to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

100. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and NKCH and Meritas, on the other hand. Indeed, as set forth *supra*, NKCH and Meritas recognized the importance of data security and the privacy of NKCH's and Meritas's patients' PII/PHI. Had Plaintiff and Class members known that NKCH and Meritas would not adequately protect their PII/PHI, they would not have received healthcare or other services from NKCH and Meritas.

101. Plaintiff and Class members performed their obligations under the implied contract when they provided NKCH and Meritas with their PII/PHI and paid for healthcare or other services from NKCH and Meritas.

102. NKCH and Meritas breached their obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, including by ensuring companies they contract with implement and maintain reasonable security measures to protect PII/PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

103. NKCH's and Meritas's breach of their obligations of their implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

104. Plaintiff and all other Class members were damaged by NKCH's and Meritas's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

COUNT VI
UNJUST ENRICHMENT
Against All Defendants

105. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

106. This claim is pleaded in the alternative to the breach of implied contract claim.

107. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid to NKCH and Meritas for healthcare services, which NKCH and Meritas used in turn to pay for PJA's services, and through the provision of their PII/PHI.

108. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate billing services and services provided to NKCH and Meritas.

109. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

110. Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security procedures for themselves that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

111. Plaintiff and Class members have no adequate remedy at law.

112. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT VII
VIOLATIONS OF THE MISSOURI MERCHANDISING PRACTICES ACT
Mo. Rev. Stat. § 407.20 *et seq.* ("MMPA")
Against Meritas Only

113. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

114. This claim is brought by Plaintiff on behalf of all Class members who provided their PII/PHI to Meritas against Meritas only.

115. Meritas offers, and continues to offer, healthcare and related services in the State of Missouri.

116. Plaintiff and other Class members purchased and received healthcare services from Meritas for personal, family, or household purposes.

117. Meritas engaged in unlawful and unfair practices in violation of the MMPA by failing to, or contracting with companies that failed to, implement and maintain reasonable security measures to protect and secure their patients' PII/PHI in a manner that complied with applicable laws, regulations, and industry standards, including by ensuring the third parties they contract with and share PII/PII with implement and maintain reasonable security measures to protect and secure PII/PHI.

118. As a result of the Data Breach, Plaintiff and Class members have lost property in the form of their PII/PHI. Further, Meritas's failure to adopt reasonable practices in protecting and safeguarding its patients' PII/PHI will force Plaintiff and other Class members to spend time or money to protect against imminent identity theft.

119. Plaintiff and Class members are now at a higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Meritas's practice of collecting and sharing PII/PHI with third parties without ensuring those third parties have appropriate and reasonable safeguards in place to protect such information.

120. Plaintiff and all other Class members were damaged by Meritas's unfair and deceptive trade practices because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

121. Plaintiff seeks all relief authorized under the MMPA, including attorney's fees and such equitable relief as the Court deems proper to protect Plaintiff and Class members from Defendants' unlawful actions as describe herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in his favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

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

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

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

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

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

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Petition so triable.

Dated: January 10, 2024

Respectfully submitted,

/s/ John S. Steward
John S. Steward (MO Bar Number 45932)
STEWARD LAW FIRM, LLC
14824 West Clayton Road, Suite 24
Chesterfield, MO 63017
Tel: 314-504-0979
Fax: 314-594-5950
js@molawgroup.com

Ben Barnow*
Anthony L. Parkhill*

BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice forthcoming*

ClassAction.org
