UNITED STATES DISTRICT COURT
SOUTHERN DISRICT OF OHIO
EASTERN DIVISION

JASON MCCUMBERS, for himself and on behalf of all others similarly situated, Plaintiff, v. MARIETTA AREA HEALTH CARE, INC., dba MEMORIAL HOSPITAL SYSTEM., Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jason McCumbers ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant Marietta Area Health are, Inc. dba Memorial Hospital System (hereinafter known as "MHS" or "Defendant"), an Ohio corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out the recent targeted cyberattack against Defendant MHS that allowed a third party to access Defendant MHS's computer systems and data, resulting in the compromise of highly sensitive personal information belonging to hundreds of thousands of current and former patients (the "Data Breach"). Because of the Data Breach, Plaintiff and approximately 216,478 Class Members[1] suffered ascertainable losses in the form of the loss of

[1] *See* Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/e7861ebb-6f43-4fe7-9619-25762e3be35d.shtml (last visited Jan. 24, 2022).

the benefit of their bargain, out- of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the imminent risk of future harm caused by the compromise of their sensitive personal information, including Social Security numbers.

2. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to MHS, its officials and agents—was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes names, Social Security numbers, medical/treatment information, health insurance information,[2] and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and protected health information ("PHI") that Defendant collected and maintained (collectively the "Private Information").

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

5. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take

steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

6. In addition, MHS and its employees failed to properly monitor the computer network and IT systems that housed the Private Information.

7. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that MHS collected and maintained is now in the hands of data thieves.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

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

10. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

11. By his Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

12. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

13. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*; (iii) invasion of privacy; (iv) breach of express contract; (v) breach of implied contract, (vi) breach of fiduciary duty, and (vii) unjust enrichment.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and Plaintiff Jason McCumbers and Members of the proposed Class are citizens of states different from Defendant.

15. The Southern District of Ohio has personal jurisdiction over Defendant because Defendant is headquartered in this District and Defendant conducts substantial business in Ohio and this District.

16. Venue is proper in this Court pursuant to 28 U.S.C. §1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District.

PARTIES

17. Plaintiff Jason McCumbers is, and at all times mentioned herein was, an individual citizen of the State of West Virginia residing in Parkersburg, West Virginia. Plaintiff was notified of the Data Breach and his Private Information being compromised upon receiving a data breach

notice letter dated January 10, 2022.[3]

18. Defendant Marietta Area Health Care, Inc. is a domestic corporation organized under the laws of the State of Ohio with its principal place of business located at 401 Matthew Street, Marietta, Ohio 45750.

DEFENDANT'S BUSINESS

19. MHS is a health system comprised of a network of hospitals, emergency departments and outpatient service sites including: Marietta Memorial Hospital, Sistersville General Hospital, Selby General Hospital, Physicians Care Express; Marietta Health Care Physicians, Inc., Memorial Health Foundation, Marietta Occupational Health Partners, and Marietta Home Health Services & Hospice.[4]

20. MHS employs over 2,700 employees, including 325 providers representing 64 clinics. The system in total works with over 500 physicians representing over 40 specialties.[5]

21. On information and belief, in the ordinary course of rendering healthcare care services, MHS requires patients (including Plaintiff and Class members) to provide sensitive personal and private information such as:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification; and
- Other information that may be deemed necessary to provide care.

---

[4] *See* https://www.linkedin.com/company/memorial-health-system-ohio/ (last visited Jan. 24, 2022); *see also* https://www.facebook.com/MHSystem/ (last visited Jan. 24, 2022).
[5] *See* https://www.facebook.com/MHSystem/ (last visited Jan. 24, 2022).

22. Plaintiff McCumbers did in fact provide his PII and PHI to Defendant, as a prerequisite to receiving treatment and care from Defendant.

23. Additionally, MHS may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patients' health plan(s), close friends, and/or family Members.

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

25. On information and belief, MHS provides each of its patients (including Plaintiff) with a HIPAA compliant notice titled "Notice of Privacy Practices" (the "Privacy Notice") that explains how it handles patients' sensitive and confidential information.[6] The Privacy Notice is posted on Defendant's website[7] and, upon information and belief, provided to each patient (including Plaintiff) prior to receiving treatment or services, and is provided to every patient upon request.

26. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, MHS promises to, among other things: keep patients' PHI private; inform patients of its legal duties and comply with laws protecting patients' PHI; only use and release patients' health information for approved reasons; provide adequate notice to patients if their Private Information is disclosed without authorization; and adhere to the terms outlined in the Privacy Notice.[8]

[6] *See* https://mhsystem.org/noticeofprivacypractice (last visited Jan. 24, 2022).
[7] *Id*.
[8] *Id*.

27. Defendant's Privacy Notice, provides, in relevant parts, the following:

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

How We May Use and Disclose Medical Information About You

For Treatment: We may use medical information about you to provide you with medical treatment or services. We may disclose medical information about you t0 doctors, nurses, technicians, or others who need to know about you to provide quality patient care. This information may be disclosed through information we record in your medical record or verbally between health care provides, We a will also provide other medical facilities with information about you and your diagnosis which they will need in order to treat you.

For Payment: We may use and disclose medical information about you so that treatment and services you received may be billed and payment may be collected from you, an insurance company or a third party. Fore ample, we may need to give your insurance company information about a procedure we performed so we can be paid for the procedure.

For Health Care Operations: We may use and disclose medical information about you for operational purposes. For example, your health information may be disclosed to members of the medical staff, risk or quality improvement personnel, and others or evaluate the performance of our staff, assess the quality of care, learn how to improve our facility and services.

Appointment. We may use your information to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you.

Fund Raising. Memorial Health Foundation may use your information to contact you to raise funds for Memorial Health System and its health related activities. We would only release contact information such as your name, address and phone number and the dates your received treatment or services at the hospital. If you do not want the Foundation to contact you for fundraisng efforts, you must notify the Memorial Health Foundation Office.

Hospital Directory. We may include certain limited information

> about you in the hospital directory while you are a patient at the hospital. This information may include your name, location in the hospital, your general condition (undetermined, good, fair, serious, critical) and your religious affiliation. [9]

28. With regard to a patient's right to receive notice if a breach occurs, the Privacy Notice provides that "[Memorial] will notify you of certain breaches or the inappropriate use or release of your information."[10]

29. Defendant also acknowledges that it is "required to maintain the privacy of protected health information."[11]

30. As a condition of receiving and purchasing healthcare services and goods from Defendant, MHS requires that its patients, such as Plaintiff and Class Members, entrust it with highly sensitive personal information.

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

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

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

THE CYBERATTACK

34. On August 14, 2021, MHS identified the presence of malware on certain servers

[9] *Id.*
[10] *Id.*
[11] *Id.*

in its environment. Upon review, MHS determined that it was the victim of a targeted Data Breach.

35. After discovering the incident, Defendant commenced an investigation to determine the full nature and scope of the incident and to secure its network.

36. On September 17, 2021, nearly a month after the Data Breach, the investigation revealed that the cyberattack enabled an unauthorized actor to gain access to certain systems on Defendant's network "on or about July 10, through August 15, 2021," allowing unauthorized access to continue for nearly an entire month.

37. The investigation revealed that Private Information was accessed and encrypted without authorization, including patients' names, Social Security numbers, medical/treatment information, and health insurance information.

38. The Private Information contained in the files accessed by hackers was not encrypted.

39. Upon information and belief, the Data Breach was targeted at Defendant due to its status as a healthcare entity that collects, creates, and maintains both PII and PHI.

40. Upon information and belief, the targeted Data Breach was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients, like Plaintiff and the Class Members.

41. Because of the Data Breach, data thieves were able to gain access to and hold hostage Defendant's IT systems and, were able to compromise, access, and acquire the protected Private Information of Plaintiff and Class Members.

42. While MHS stated in its "Notice of Security Incident" letters, sent to Plaintiff's and Class members, that it learned of the Data Breach on August 14, 2021, MHS did not begin notifying impacted patients, such as Plaintiff and Class Members, until January 19, 2022 – more

than five months after discovering the Data Breach. MHS's delay in notifying its customers affected by the Data Breach violated the provisions of Ohio's Security Breach Notification Act, ORC 1349.19, which required MHS to notify consumers as quickly as possible but no later than 45 days after the breach is discovered.

43. What is more, in the notices that MHS belatedly provided, MHS openly admitted in the Notice of Data Breach that the Private Information of Plaintiff and Class Members that was accessed without authorization by hackers was indeed "acquired" by the cyberthieves who perpetrated the Data Breach. This means that not only did the cybercriminals view and access the Private Information without authorization, but they also removed Plaintiff's and Class Members' Private Information from MHS's network.

44. Due to Defendant's incompetent security measures, Plaintiff and the Class Members now face an increased risk of fraud and identity theft and must deal with that threat forever.

45. Plaintiff believes his Private Information was both stolen in the Data Breach (a fact admitted by Defendant in its Notice of Data Breach where Defendant states that the cybercriminals "acquired" the data) and is still in the hands of the hackers. Plaintiff further believes his Private Information was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals who perpetrate cyberattacks of the type that occurred here.

46. Many ransomware variants that have been used recently have expanded to include data exfiltration.[12]

47. Defendant had obligations created by HIPAA, contract, industry standards,

[12] *See* https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/

common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

48. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

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

50. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[13] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[14] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[15]

51. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and

[13] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[14] *Id*.
[15] *Id*.

BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

52. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[16]

53. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[17]

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

Defendant Fails to Comply with FTC Guidelines

55. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

56. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any

[16] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Jan. 25, 2022).
[17] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

security problems.[18]The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[19]

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

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

59. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

60. Defendant failed to properly implement basic data security practices.

[18] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 15, 2021).
[19] *Id*.

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

62. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

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

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

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

66. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

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

68. HIPAA requires covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

69. Covered entities (including Defendant MHS) must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

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

71. A Data Breach such as the one Defendant experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

A breach under the HIPAA Rules is defined as, "...the acquisition, access, use,

> or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

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

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[20]

73. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate MHS failed to comply with safeguards and standards of care mandated by HIPAA regulations.

DEFENDANT'S NEGLIGENT ACTS AND BREACH

74. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect patients' Private Information;

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

[20] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4.

d. Failing to train its employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's networks, and to maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R.

§ 164.306(a)(1);

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

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

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

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. §

164.306(a)(2);

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

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

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

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

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

p. Failing to adhere to industry standards for cybersecurity.

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

would protect against cyberattacks like the ransomware intrusion here, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access, and hold hostage, MHS's IT systems, and which contained unsecured and unencrypted Private Information.

76. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with Defendant.

Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

77. Data breaches at healthcare providers like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

78. For instance, loss of access to patient histories, charts, images and other information forces providers to limit or cancel patient treatment because of the disruption of service.

79. This leads to a deterioration in the quality of overall care patients receive at facilities affected by data breaches.

80. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[21]

81. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[22]

[21] *See* Nsikan Akpan, Ransomware and Data Breachs Linked to Uptick in Fatal Heart Attacks, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart- attacks (last visited Jan. 25, 2022).

[22] *See* Sung J. Choi et al., Cyberattack Remediation Efforts and Their Implications for Hospital Quality, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-

82. Similarly, data breach incidents cause patients issues with receiving care that rise above the level of mere inconvenience. The issues that patients encounter as a result of such incidents include, but are not limited to:

a. rescheduling their medical treatment;

b. finding alternative medical care and treatment;

c. delaying or foregoing medical care and treatment; and

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. inability to access their medical records.[23]

83. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[24]

84. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track

6773.13203 (last visited Jan. 25, 2022).

[23] *See, e.g.,* Lisa Vaas, Cyberattacks Paralyze, and Sometimes Crush, Hospitals, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals//___(last visited Jan. 25, 2022); Jessica David, Data Breaches Will Cost Healthcare $4B in 2019. Threats Outpace Tech, Health IT Security (Nov. 5, 2019), https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech - :~:text=November 05, 2019 - Healthcare data,per each breach patient record (last visited Jan. 25, 2022).

[24] *See* U.S. Gov. Accounting Office, GAO-07-737, "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" (GOA, 2007). Available at https://www.gao.gov/new.items/d07737.pdf. (last visited Jan. 25, 2022).

the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

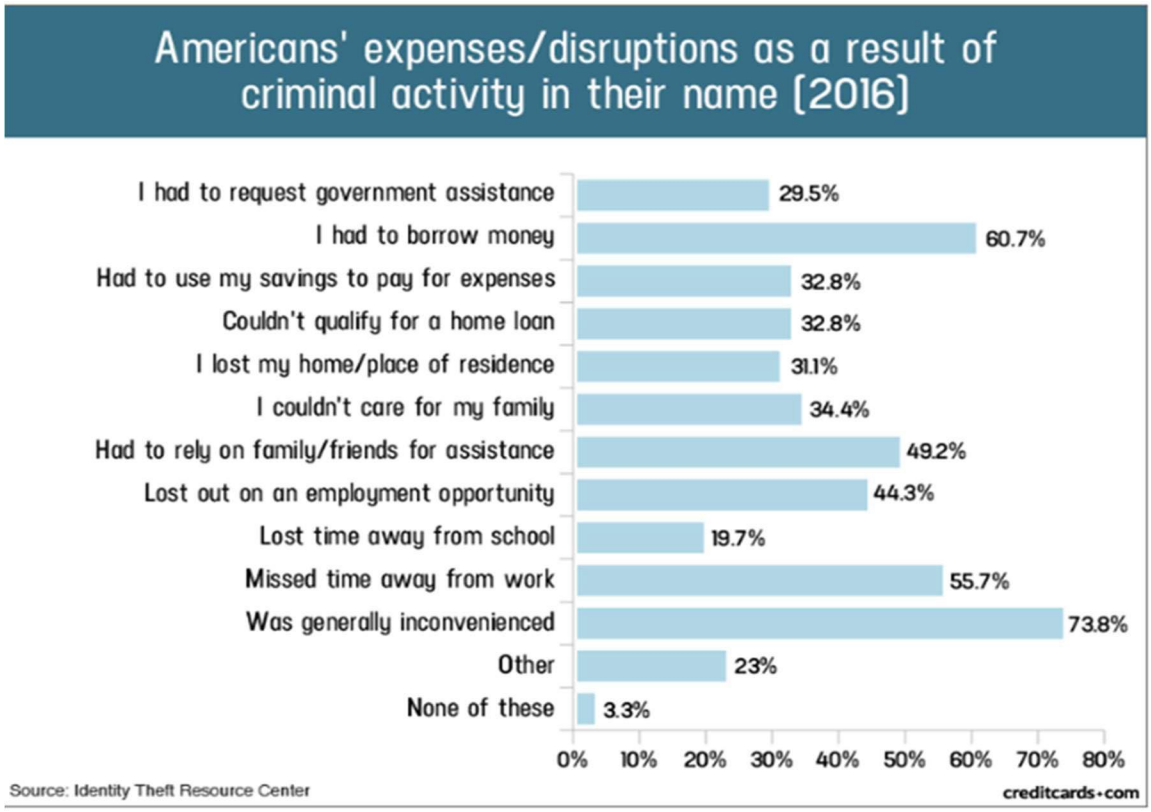
85. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[25]

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

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

[25] *See* IdentityTheft.gov, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 25, 2022).

88. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[26]



89. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.[27]

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

---

[26] *See* Jason Steele, Credit Card and ID Theft Statistics, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php. (last visited Jan. 25, 2022).

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

91. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[28]

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

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

94. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

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

[28] *See* Federal Trade Commission, What to Know About Medical Identity Theft, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft identity-theft (last visited Jan. 25, 2022).

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

97. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

98. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[29] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

99. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[30] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[31]Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

100. Moreover, it is not an easy task to change or cancel a stolen Social Security

---

[29] *See* Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 25, 2022).

[30] Identity Theft and Your Social Security Number, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 25, 2022).

[31] *Id*. at 4.

number.

101. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

102. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

103. Medical information is especially valuable to identity thieves.

104. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[32] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[33]

105. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

106. For this reason, Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

[32] *See* Omri Toppol, Email Security: How You Are Doing It Wrong & Paying Too Much, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last visited Jan. 25, 2022).
[33] *See* Vaas, Cyberattacks, *supra*, n. 28.

Plaintiff's and Class Members' Damages

107. To date, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

108. Defendant has merely offered Plaintiff and Class Members fraud and identity monitoring services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach. What is more, Defendant places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

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

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

111. In or around January 10, 2022, Plaintiff received notice from MHS that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff's Private Information, including his name, Social Security number, medical treatment information, and health insurance information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

112. Upon information and belief, Plaintiff's telephone number and email address were included in the medical treatment information and/or the health insurance information that was compromised in this Data Breach.

113. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the

impact of the Data Breach after receiving the data breach notification letter, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by MHS. Plaintiff now spends approximately one hour per day reviewing his bank accounts and other sensitive accounts for irregularities.

114. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including increased anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

115. Subsequent to the Data Breach, Plaintiff experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls and spam emails, all of which appear to be placed with the intent to obtain personal information in order to commit identity theft by way of a social engineering

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

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

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

119. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that MHS obtained from Plaintiff; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

120. Plaintiff and Class Members were also injured by and suffered benefit-of-the-bargain damages from this Data Breach. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of MHS's computer property and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

121. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out- of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

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

d. Spending time on the phone with or at financial institutions, healthcare

providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

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

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

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

CLASS ACTION ALLEGATIONS

123. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class").

124. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> All persons who utilized MHS's services, whose Private Information was maintained on MHS's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "Class").

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

126. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately 216,478 individuals whose sensitive data was compromised in the Data Breach.

127. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

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

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

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

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

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

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

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

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

i. Whether Plaintiff and Class Members suffered legally cognizable injuries as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached a fiduciary duty to Plaintiff and Class Members;

l. Whether Defendant breached express or implied contracts with Plaintiff and Class Members ;

m. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

n. Whether Defendant failed to provide notice of the Data Breach ina timely manner; and,

o. Whether Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages, and/or injunctive relief.

128. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

129. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

130. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the

same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

131. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

132. 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.

CAUSES OF ACTION

COUNT ONE

Negligence
(On Behalf of Plaintiff and the Class)

133. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 132 above as if fully set forth herein.

134. Defendant required patients, including Plaintiff and Class Members, to submit non-

public Private Information in the ordinary course of rendering healthcare services.

135. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they 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.

136. 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 systems and networks, and the personnel responsible for them, adequately protected the Private Information.

137. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, state law, and common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach and data breach.

138. Defendant's duty to use reasonable security measures under HIPAA required Defendant 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 case constitutes "protected health information" within the meaning of HIPAA.

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

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

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

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

b. Failing to adequately monitor the security of its IT system;

c. Failing to ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Failure to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information; and

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

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

143. It was therefore foreseeable that the failure to adequately safeguard Class Members'

Private Information would result in one or more types of injuries to Class Members.

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

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

COUNT TWO

Negligence Per Se
(On Behalf of Plaintiff and All Class Members)

146. Plaintiff re-alleges and incorporate by reference Paragraphs 1 through 132 above as if fully set forth herein.

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

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

149. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

150. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant had a duty to protect the security and confidentiality of Plaintiff's and Class Members' Private

Information.

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

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

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

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

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

COUNT THREE

Invasion of Privacy
(On Behalf of Plaintiff and the Class)

156. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 132 as if fully set forth herein.

157. The State of Ohio recognizes the tort of Invasion of Privacy:

> The elements of an invasion-of-privacy claim are (1) intrusion upon the plaintiff's seclusion or solitude, or into his or her private affairs, (2) public

> disclosure of embarrassing private facts about the plaintiff, (3) publicity that places the plaintiff in a false light in the public eye, or (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness

Georgetown of the Highlands Condo. Owners' Ass'n v. Nsong, 2018-Ohio-1966, 113 N.E.3d 192

Doe v. Mills, 212 Mich. App. 73, 80, 536 N.W.2d 824, 828 (1995).

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

159. Defendant's conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion under common law.

160. By intentionally failing to keep Plaintiff's and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and Class Members' privacy by:

161. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person, and intentionally causing anguish or suffering to Plaintiff and Class Members.

162. Defendant knew that an ordinary person in Plaintiff's or a Class Member's position would consider Defendant's intentional actions highly offensive and objectionable.

163. Defendant invaded Plaintiff and Class Members' right to privacy and intruded into Plaintiff's and Class Members' seclusion by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

164. Defendant intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their Private information without their informed, voluntary,

affirmative, and clear consent.

165. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

166. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seek an award of damages on behalf of himself and the Class.

COUNT FOUR

Breach of Express Contract
(On Behalf of Plaintiff and the Class)

167. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 132 above as if fully set forth herein.

168. Plaintiff and Members of the Class allege that they entered into valid and enforceable express contracts with Defendant.

169. The valid and enforceable express contracts that Plaintiff and Class Members entered into with Defendant include Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathers on its own from disclosure.

170. Under these express contracts, Defendant and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class

Members; and (b) protect Plaintiff's and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

171. Both the provision of healthcare and the protection of Plaintiff's and Class Members' PII/PHI were material aspects of these contracts.

172. At all relevant times, Defendant expressly represented in its Privacy Notice that it would, among other things: A) "maintain the privacy of protected information;" B) "release the minimum amount of your information necessary" and; C) "obtain your written authorization to use or disclose your health information for reasons other than those described in this notice."

173. At least one of these promises embodied in the Privacy Notice (the promise to "release the minimum amount of your information necessary") is not a promise required to be in the Privacy Notice by HIPAA regulations.

174. Defendant's express representations, including, but not limited to, express representations found in its Privacy Notice, formed an express contract requiring Defendant's to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII/PHI.

175. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their PII/PHI associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect PII/PHI is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entered into these contracts with Defendant and/or its affiliated healthcare providers without an

understanding that their PII/PHI would be safeguarded and protected.

176. A meeting of the minds occurred, as Plaintiff and Members of the Class provided their PII/PHI to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their PII/PHI.

177. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their PII/PHI.

178. Defendant materially breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

179. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiff's and Class Members' PII/PHI as evidenced by its notifications of the Data Breach to Plaintiff and approximately 216,478 Class Members. Specifically, Defendant did not comply with industry standards, or otherwise protect Plaintiff's and the Class Members' PII/PHI, as set forth above.

180. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

181. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

182. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

183. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the compromise of their PII/PHI, the loss of control of their PII/PHI, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

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

COUNT FIVE

Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

185. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 132 as if fully set forth herein.

186. When Plaintiff and Class Members provided their Private Information to MHS in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

187. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offer and provided their Private Information to Defendant.

188. In entering into such implied contracts, Plaintiff and Class Members reasonably

believed and expected that Defendant's data security practices complied with relevant federal and state laws and regulations and were consistent with industry standards.

189. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendant include Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathers on its own from disclosure.

190. Under these implied contracts, Defendant and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

191. Both the provision of healthcare and the protection of Plaintiff's and Class Members' PII/PHI were material aspects of these implied contracts.

192. At all relevant times, Defendant expressly represented in its Privacy Notice that it would, among other things: A) "maintain the privacy of protected information;" B) "release the minimum amount of your information necessary" and; C) "obtain your written authorization to use or disclose your health information for reasons other than those described in this notice."

193. At least one of these promises embodied in the Privacy Notice (the promise to "release the minimum amount of your information necessary") is not a promise required to be in the Privacy Notice by HIPAA regulations.

194. Defendant's express representations, including, but not limited to, express representations found in its Privacy Notice, memorialized the mutual assent and meeting of the minds between Plaintiff, Class Members, and Defendant, and is part of the implied contract

requiring Defendant's to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII/PHI.

195. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their PII/PHI associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect PII/PHI is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entered into these implied contracts with Defendant and/or its affiliated healthcare providers without an understanding that their PII/PHI would be safeguarded and protected.

196. A meeting of the minds occurred, as Plaintiff and Members of the Class provided their PII/PHI to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their PII/PHI.

197. Plaintiff and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

198. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

199. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

200. Through its myriad failures to provide the promised level of data security and

protection alleged previously herein, Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

201. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

202. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of MHS's computer property and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for and contractually agreed to.

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

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

COUNT SIX

Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

205. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 132 as if fully set forth herein.

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

Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a data breach and disclosure; and (3) maintain complete and accurate records of what patient information (and where) Defendant did and does store.

207. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of this relationship, in particular, to keep secure the Private Information of its patients.

208. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to adequately protect against cybersecurity events and give notice of the Data Breach in a reasonable and practicable period of time.

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

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

211. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

212. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

213. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by

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

214. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

215. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

216. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

217. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

218. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

219. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. §

164.530(b) and 45 C.F.R. § 164.308(a)(5).

220. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

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

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

223. As a direct and proximate result of Defendant's breaching its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury

and/or harm, and other economic and non-economic losses.

COUNT SEVEN

Unjust Enrichment
(On Behalf of Plaintiff and the Class)

224. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 132 as if fully set forth herein.

225. This count is plead in the alternative to Counts 3 and 4 (breach of express and breach of implied contract).

226. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant money for healthcare services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' PII and PHI, and by providing Defendant with their valuable PII and PHI.

227. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach.

228. Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

230. Defendant acquired the monetary benefit and PII and PHI through inequitable

means in that it failed to disclose the inadequate security practices previously alleged.

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

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

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

234. 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.

235. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and

Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a Class action and appointing Plaintiff and his counsel to represent the Class;

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

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

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

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

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

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

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

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

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: January 27, 2022

Respectfully Submitted,

By: *Terence R. Coates*
Terence R. Coates (0085579)
MARKOVITS STOCK & DEMARCO
119 E. Court St.
Cincinnati, OH
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
Email: tcoates@msdlegal.com

Gary E. Mason (pro hac vice forthcoming)
David K. Lietz (pro hac vice forthcoming)
MASON LIETZ & KLINGER LLP
5101 Wisconsin Ave., NW, Ste. 305
Washington, DC 20016
Telephone: (202) 640.1160
Email: gmason@masaonllp.com
Email: dlietz@masonllp.com

Gary M. Klinger (pro hac vice forthcoming)
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606 Telephone: (202) 975-0477
Email: gklinger@masonllp.com

Attorneys for Plaintiff and the Proposed Class

JS 44 (Rev. 02/19)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

JASON MCCUMBERS, for himself and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Wood County, WV
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
MARKOVITS STOCK & DEMARCO LLC
3825 Edwards Rd, Suite 650
Cincinnati, OH 45209

DEFENDANTS

MARIETTA AREA HEALTH CARE, INC., dba MEMORIAL HOSPITAL SYSTEM.,

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	❒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	☒ 4
Citizen of Another State	☒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ❒ 110 Insurance
- ❒ 120 Marine
- ❒ 130 Miller Act
- ❒ 140 Negotiable Instrument
- ❒ 150 Recovery of Overpayment & Enforcement of Judgment
- ❒ 151 Medicare Act
- ❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ❒ 153 Recovery of Overpayment of Veteran's Benefits
- ❒ 160 Stockholders' Suits
- ❒ 190 Other Contract
- ❒ 195 Contract Product Liability
- ❒ 196 Franchise

REAL PROPERTY
- ❒ 210 Land Condemnation
- ❒ 220 Foreclosure
- ❒ 230 Rent Lease & Ejectment
- ❒ 240 Torts to Land
- ❒ 245 Tort Product Liability
- ❒ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ❒ 310 Airplane
- ❒ 315 Airplane Product Liability
- ❒ 320 Assault, Libel & Slander
- ❒ 330 Federal Employers' Liability
- ❒ 340 Marine
- ❒ 345 Marine Product Liability
- ❒ 350 Motor Vehicle
- ❒ 355 Motor Vehicle Product Liability
- ❒ 360 Other Personal Injury
- ❒ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ❒ 365 Personal Injury - Product Liability
- ❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ❒ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ❒ 370 Other Fraud
- ❒ 371 Truth in Lending
- ☒ 380 Other Personal Property Damage
- ❒ 385 Property Damage Product Liability

CIVIL RIGHTS
- ❒ 440 Other Civil Rights
- ❒ 441 Voting
- ❒ 442 Employment
- ❒ 443 Housing/ Accommodations
- ❒ 445 Amer. w/Disabilities - Employment
- ❒ 446 Amer. w/Disabilities - Other
- ❒ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ❒ 463 Alien Detainee
- ❒ 510 Motions to Vacate Sentence
- ❒ 530 General
- ❒ 535 Death Penalty

Other:
- ❒ 540 Mandamus & Other
- ❒ 550 Civil Rights
- ❒ 555 Prison Condition
- ❒ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ❒ 625 Drug Related Seizure of Property 21 USC 881
- ❒ 690 Other

LABOR
- ❒ 710 Fair Labor Standards Act
- ❒ 720 Labor/Management Relations
- ❒ 740 Railway Labor Act
- ❒ 751 Family and Medical Leave Act
- ❒ 790 Other Labor Litigation
- ❒ 791 Employee Retirement Income Security Act

IMMIGRATION
- ❒ 462 Naturalization Application
- ❒ 465 Other Immigration Actions

BANKRUPTCY
- ❒ 422 Appeal 28 USC 158
- ❒ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 835 Patent - Abbreviated New Drug Application
- ❒ 840 Trademark

SOCIAL SECURITY
- ❒ 861 HIA (1395ff)
- ❒ 862 Black Lung (923)
- ❒ 863 DIWC/DIWW (405(g))
- ❒ 864 SSID Title XVI
- ❒ 865 RSI (405(g))

FEDERAL TAX SUITS
- ❒ 870 Taxes (U.S. Plaintiff or Defendant)
- ❒ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ❒ 375 False Claims Act
- ❒ 376 Qui Tam (31 USC 3729(a))
- ❒ 400 State Reapportionment
- ❒ 410 Antitrust
- ❒ 430 Banks and Banking
- ❒ 450 Commerce
- ❒ 460 Deportation
- ❒ 470 Racketeer Influenced and Corrupt Organizations
- ❒ 480 Consumer Credit
- ❒ 485 Telephone Consumer Protection Act
- ❒ 490 Cable/Sat TV
- ❒ 850 Securities/Commodities/ Exchange
- ❒ 890 Other Statutory Actions
- ❒ 891 Agricultural Acts
- ❒ 893 Environmental Matters
- ❒ 895 Freedom of Information Act
- ❒ 896 Arbitration
- ❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ❒ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding | ❒ 2 Removed from State Court | ❒ 3 Remanded from Appellate Court | ❒ 4 Reinstated or Reopened | ❒ 5 Transferred from Another District *(specify)* | ❒ 6 Multidistrict Litigation - Transfer | ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)(2), Class Action Fairness Act

Brief description of cause:
Privacy Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE Graham; Morrison DOCKET NUMBER 2:22-CV-221; 2:22-CV-184

DATE
01/27/2022

SIGNATURE OF ATTORNEY OF RECORD
/s/ Terence R. Coates

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

Print Save As... Reset

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket. **PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

ClassAction.org
