**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF OHIO**
**EASTERN DIVISION**

| | |
|---|---|
| **KATHLEEN TUCKER,** on behalf of themselves and all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>**MARIETTA AREA HEALTH CARE INC. D/B/A MEMORIAL HEALTH SYSTEM,**<br><br>Defendant. | Case No.<br><br>Judge<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

## CLASS ACTION COMPLAINT

Plaintiff Kathleen Tucker, individually and on behalf of all others similarly situated, brings this action against Defendant Marietta Area Health Care Inc. d/b/a Memorial Health System (hereinafter known as "Memorial Health" 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 her own actions, the investigation of her counsel, and the facts that are a matter of public record.

## NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") on Memorial Health's network that resulted in unauthorized access to customer data. As a result of the Data Breach, Plaintiff and approximately 216,478 Class Members[1] suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/e7861ebb-6f43-4fe7-9619-25762e3be35d.shtml (Last visited Jan. 19, 2022).

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

3. Information compromised in the Data Breach includes names, dates of birth, medical record numbers, patient account numbers, Social Security Numbers, "PII"), and medical and treatment information ("PHI"), The PII and PHI that Defendant Memorial Health collected and maintained will be collectively referred to as 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 they 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 cyberattacks. Upon information and belief, the mechanism of the cyberattack 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. Plaintiff and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Memorial Health collected and maintained is now in the hands of data thieves.

7. 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.

8. 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.

9. 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.

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

11. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive 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.

12. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, and (iii) breach of implied contract; and (iv) unjust enrichment.

## THE PARTIES

13. Plaintiff Kathleen Tucker is a natural person, resident and a citizen of the State of West Virginia. She has lived in West Virginia since 1979 and has no intention of moving to a different state in the immediate future. She is registered to vote in West Virginia as well. Plaintiff Tucker is acting on her own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Tucker's PII and PHI and owed her a legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure. Plaintiff Tucker would not have entrusted her PII and PHI to Defendant had she known that Defendant failed to maintain adequate data security. Plaintiff Tucker's PII and PHI was compromised and disclosed as a result of Defendant's inadequate data security and the Data Breach.

## JURISDICTION AND VENUE

14. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Plaintiff (and many members of the class) and Defendant are citizens of different states.

15. This Court has general personal jurisdiction over Memorial Health because Memorial's principal place of business is, and does regularly conduct business, in Marietta, Ohio.

16. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Memorial Health conducts substantial business in this District.

## DEFENDANT'S BUSINESS

17. Memorial Health provides comprehensive medical care throughout the Marietta and surrounding region.

18. Defendant Memorial Health "employs over 2,700 employees, including 325 providers representing 64 clinics."[2] Memorial Health represents that it "strive[s] to deliver quality, affordable care with an additional focus on medical and community service."[3]

19. Defendant Memorial Health claims it "is dedicated to providing you with healthcare information and referral services of the highest quality, whole at the same time protecting your privacy."[4]

20. Defendant Memorial Health further claims it is "very concerned with the security of your personally identifiable information and take[s] great care in providing secure transmission of your information from your computer to our services."[5] Defendant also states that "[o]nce we receive your information, we take appropriate steps that we believe are reasonable to protect the security of your data on our system."[6]

21. On information and belief, in the ordinary course of rendering healthcare care services, Memorial Health requires its patients and customers 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;

[2] Mission and Vison, Memorial Health, https://mhsystem.org/missionandvision (Last visited Jan. 19, 2022).
[3] *Id*.
[4] Web Site Privacy Notice, Memorial Health, https://mhsystem.org/websiteprivacy (Last visited Jan. 19, 2022).
[5] *Id*.
[6] *Id*.

- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification;
- Employment information, and;
- Other information that may be deemed necessary to provide care.

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

23. On information and belief, Memorial Health provides each of its patients and customers with a HIPAA compliant notice titled "Memorial Health of Ohio Notice of Privacy Practices" (the "Privacy Notice") that explains how they handle customers' sensitive and confidential information.[7]

24. The Privacy Notice is posted in Defendant's offices, provided to every customer upon request, and a "summary" is posted on Defendant's website.[8]

25. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its customers, Memorial Health, upon information and belief, promises to, among other things: keep customers' protected health information (PHI) private; comply with healthcare industry standards related to data security and Private Information; inform customers and patients of its legal duties and comply with all federal and state laws protecting customers' and patient's Private Information ; only use and release customers' Private Information

[7] *See Notice of Privacy Practices*, Memorial Health of Ohio, https://mhsystem.org/noticeofprivacypractice (Last visited Jan. 18, 2022).
[8] *Id*.

for reasons that relate to the customers or patients medical care and treatment; provide adequate notice to customers if their Private Information is disclosed without authorization; and adhere to the terms outlined in the Privacy Notice.[9]

26. As a condition of purchasing goods and services from Defendant, Memorial Health requires that its customers entrust it with Private Information.

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

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

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

## THE CYBERATTACK AND DATA BREACH

30. On August 14, 2021, Memorial Health identified the presence of malware on the Marietta servers that was impacting all three Memorial Health hospitals in Ohio and West Virginia.

31. The Data Breach resulted in a ransomware group encrypting the Hospital System and shutting down the IT systems.[10]

[9] https://mhsystem.org/noticeofprivacypractice (Last visited on Jan. 19, 2022).
[10] https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/

32. Emergency protocols were implemented that forced the medical staff off-line and to work with paper charts until the system could be restored thereby placing patients at risk for medical errors. With no access to radiology or electronic charts, Memorial Health decided to divert emergency patients to other hospitals. Moreover, all urgent surgical appointments and radiology examination were cancelled.[11]

33. It was reported that Hive ransomware, a known data security threat group, was responsible for the attack. Hive has a common course of conduct of exfiltrating and stealing data prior once the data is accessed. Hive maintains a leak site on the Dark Web that is used to pressure victims into paying the ransom once it obtains the sensitive information.[12] "By exfiltrating information, the attackers have more leverage to force the victim to pay the ransom in exchange for the promise to not share or leak the stolen data and to provide a decryption tool."[13]

34. Upon information and belief, Plaintiff's and class members' information was exfiltrated and stolen in the attack. Indeed, Bleeping Computer reported that evidence has been obtained that suggest databases containing the Sensitive Information were stolen in the attack.[14]

35. Memorial Health "worked with a national cybersecurity experts to resolve the impact of a cyber attack in the early morning hours of August 15, 2021."[15]

36. Through the investigation, Defendant determined that from July 10, 2021 through August 15, 2021, an unauthorized actor had "accessed certain systems within their network".[16]

---

[11] https://www.hipaajournal.com/cyberattack-forces-memorial-health-system-to-divert-patients-to-alternate-hospitals/ (Last visited Jan. 19, 2022)
[12] Id.
[13] https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/
[14] Id.
[15] *Id.*
[16] Ex.1. https://mhsystem.org/assets/documents/DataNotice.pdf (Last visited Jan. 19, 2022)

37. Furthermore, the investigation determined that the accessed systems contained sensitive information and that was accessible, unprotected and vulnerable for acquisition and/or exfiltration by the unauthorized actor.[17]

38. The type of Sensitive Information accessed by the unauthorized actor included includes names, dates of birth, medical record numbers, patient account numbers, Social Security Numbers, and medical and treatment information.[18]

39. As a result of the Data Breach, Memorial Health was required to follow "a deliberate, systematic approach to bring systems back online securely and in a manner that prioritizes [Memorial Health's] ability to provide patient care."[19] In addition, the investigation revealed that approximately 216,478 individuals were victims of the Data Breach.[20]

40. While Memorial Health stated in the "Notice of Data Security Incident" letter that August 15, 2021, Memorial Health did not begin notifying victims until January 10, 2022 – approximately five months after discovering the Data Breach.

41. Upon information and belief, and based on the type of cyber attack, along with public news reports, it is plausible and likely that Plaintiff's Private Information was stolen in the Data Breach. Plaintiff further believes her Private Information was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of all cybercriminals.

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

---

[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] https://apps.web.maine.gov/online/aeviewer/ME/40/e7861ebb-6f43-4fe7-9619-25762e3be35d.shtml

43. 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.

44. 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.

45. In light of recent high profile data breaches at other healthcare partner and provider companies, Defendant knew or should have known that their electronic records and patient and customer Sensitive Information would be targeted by cybercriminals and ransomware attack groups like Hive.

46. Indeed, cyberattacks on medical systems like Defendant have become so notorious that the 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. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[21]

47. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[22]

48. 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.

[21] *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 June 23, 2021).
[22] *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.

***Defendant Fails to Comply with FTC Guidelines***

49. 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.

50. 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 customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[23] 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.[24]

51. 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.

52. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

[23] *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 Jan. 19, 2022).
[24] *Id*.

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.

53. 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.")

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

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

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

***Defendant Fails to Comply with Industry Standards***

57. 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.

58. 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.

59. 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; training staff regarding critical points.

60. 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.

61. 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 the cyber incident and causing the data breach.

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

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

63. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

64. 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).

65. A Data Breach such as the one Defendant experienced, is 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

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

## DEFENDANT'S BREACH

67. 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 and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

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

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing PII and PHI and maintain adequate email security practices;

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 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);

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 workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces 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's 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 as discussed above.

q. Otherwise breached its duties and obligations to protect Plaintiff's and Class Members' Sensitive Information.

68. Defendant negligently and unlawfully failed to safeguard Plaintiff and Class Members' Private Information by allowing cyberthieves to access Memorial Health's computer network and systems which contained unsecured and unencrypted PII.

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

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

70. Cyberattacks and 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.

71. 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.[25]

72. 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.[26]

73. 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."[27]

74. 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

[25] *See* Nsikan Akpan, *Ransomware and Data Breaches 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.

[26] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[27] *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 (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. 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.

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

76. 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.

77. 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

[28] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 19, 2022).

issued in the victim's name.

78. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.[29]

79. 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.

80. 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."[30]

81. 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.

82. 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.

83. According to the U.S. Government Accountability Office, which conducted a study

[29] *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).

[30] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Jan. 19, 2022).

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.

84. 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.

85. 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.

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

87. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[31] 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.

88. 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.[32] 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

[31] *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/.
[32] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (Jan. 19, 2022).

unemployment benefits, or apply for a job using a false identity.[33] 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.

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

90. 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."[34]

91. 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."[35]

92. Medical information is especially valuable to identity thieves.

93. 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.[36] That

[33] *Id* at 4.
[34] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.
[35] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.
[36] *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/.

pales in comparison with the asking price for medical data, which was selling for $50 and up.[37]

94. 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.

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

***Plaintiff and Class Members' Damages***

96. 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.

97. Defendant has merely offered Plaintiff and Class Members complimentary 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.

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

99. Plaintiff's names, addresses, Social Security Number, medical and 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.

100. As a result of the Data Breach, Plaintiff Tucker has experienced a substantial increase in suspicious scam phone calls which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

[37] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

101. Since being notified of the Data Breach, Plaintiff Tucker has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

102. Following the Data Breach, Plaintiff was notified of two fraudulent charges on her Discovery Card, which was the same card she used to pay for all of her medical services, including prescriptions and any co-pays.

103. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring her accounts for fraudulent activity. She has had to change numerous accounts that contained monthly billing auto pay to protect against future theft. She also intends to sign up for identity theft monitoring with a cost of $16 per month.

104. Plaintiff's Private Information was compromised as a direct and proximate result of the Data Breach.

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

106. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

107. 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.

108. 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.

109. 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.

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

111. 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 that complied with industry standards 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 Memorial Health's computer property and Plaintiff and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for and agreed to.

112. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their medical accounts and sensitive information for misuse.

113. 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 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.

114. 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.

115. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

116. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

***Plaintiff Tucker's Experience***

117. Plaintiff Tucker received medical care and treatment at Memorial Health in the past. Upon information and belief, during the course of the visits, she was presented with standard medical forms to complete prior to her service that requested her PII and PHI, including HIPPA and privacy disclosure forms.

118. As part of her care and treatment, and as a requirement to receive Defendant's services, Plaintiff Tucker entrusted her PII, PHI, and other confidential information such as name, address, Social Security number, medical and treatment information, and health insurance information to Memorial Health with the reasonable expectation and understanding that Memorial Health would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff would not have used Memorial Health's services had she known that Memorial Health would not take reasonable steps to safeguard her sensitive PII and PHI.

119. Plaintiff also provided her discovery credit card information for payment of prescription and copays directly to Memorial or to its billing vendors.

120. In January 2022, more than five months after Memorial Health learned of the data breach, Plaintiff Tucker received a letter from Memorial Health, dated January 10, 2022, notifying her that her PII and PHI had been improperly accessed and/or obtained by unauthorized third parties. The notice indicated that Plaintiff Tucker's PII and PHI, including her full name, address,

Social Security number, medical and treatment information, and health insurance information was compromised as a result of the Data Breach.[38]

121. As a result of the Data Breach, Plaintiff Tucker 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, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. She has also attempted to mitigate the risk of identity theft by changing passwords, cancelling credit and debit cards. She has had to change numerous accounts that contained monthly billing auto pay to protect against future theft. She also intends to sign up for identity theft monitoring with a cost of $16 per month.

122. Plaintiff Tucker has spent approx. 10 hours and will continue to spend valuable time Plaintiff Tucker otherwise would have spent on other activities, including but not limited to work and/or recreation.

123. Plaintiff Tucker suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII and PHI, a form of property that Memorial Health obtained from Plaintiff Tucker; (b) violation of her privacy rights;(c) the likely theft of her PII and PHI; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

124. Moreover, subsequent to the Data Breach, Plaintiff Tucker also experienced actual identity theft and fraud, including notification that fraudulent charges were made on her debit card, and a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or email messages, some of which relate to medical issues, which she did not

[38] Ex.2.

receive before the breach. .

125. As a result of the Data Breach, Plaintiff Tucker has also suffered emotional distress as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of identity theft and fraud. Plaintiff Tucker is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

126. As a result of the Data Breach, Plaintiff Tucker anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Tucker will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

## CLASS ACTION ALLEGATIONS

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

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

> All persons Memorial Health identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").
>
> All patients and/or customers Memorial Health identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Customer Sub-class").

129. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives,

attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

130. Plaintiff reserves the right to amend or modify the Class or Subclass definitions as this case progresses.

131. 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 141,149 consumers of Memorial Health whose sensitive data was compromised in Data Breach.

132. 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 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;

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

h. Whether Defendant should have discovered the Data Breach sooner;

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

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

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

m. Whether Defendant violated the consumer protection statute invoked below;

n. Whether Defendant breach implied or express contracts with Plaintiff and Class Members;

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

p. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

q. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

133. 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.

134. 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.

135. Predominance. Defendant have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff 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.

136. 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.

137. 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

### FIRST COUNT
### Negligence
### (On Behalf of Plaintiff and the Class)

138. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

139. Defendant required customers, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of rendering healthcare services.

140. 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.

141. 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.

142. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including but not limited to HIPAA, as well as 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.

143. 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.

144. 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.

145. 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.

146. 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 their networks and systems;

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

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

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

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. 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.

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

148. 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.

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

150. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their 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.

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

151. Plaintiff repeats and re-alleges each and every allegation contained the Complaint as if fully set forth herein.

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

153. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Class due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

154. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

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

156. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

157. As a direct and proximate result of Defendant's negligence per se, 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; (iv) out-of-pocket expenses associated with the prevention, detection, and

recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Class.

158. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

**THIRD COUNT**
**Breach of Implied Contract**
***(On behalf of the Plaintiff and the Class)***

159. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

160. Plaintiff and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

161. Plaintiff and the Class were required to and delivered their Sensitive Information to Defendant as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

162. Defendant accepted possession of Plaintiff's and Class Members' Sensitive Information for the purpose of providing services or Plaintiff and Class Members.

163. In accepting such information and payment for services, Plaintiff and the other Class Members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class Members' Sensitive Information.

164. In delivering their Sensitive Information to TriHealth and paying for healthcare services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the data as part of that service.

165. In their written policies and registration form, TriHealth expressly and impliedly promised to Plaintiff and Class Members that it would only disclose protected information and other Sensitive Information under certain circumstances, none of which related to a Data Breach as occurred in this matter.

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

167. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to PII or PHI also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained

agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

168. Plaintiff and the Class Members would not have entrusted their Sensitive Information to Defendant in the absence of such an implied contract.

169. Had Defendant disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members would not have provided their Sensitive Information to Defendant.

170. Defendant recognized that Plaintiff's and Class Member's personal data is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

171. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendant.

172. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their data as described herein.

173. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

## FOURTH COUNT
**Unjust Enrichment**
**(On Behalf of Plaintiff and the Class)**

174. Plaintiff repeats and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

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

176. 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.

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

178. 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 industry standards.

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

180. 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.

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

182. 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 is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII and PHI in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

183. 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.

184. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. 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 as Class Representative and her counsel as Class Counsel;

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, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

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

i) Pre- and post-judgment interest on any amounts awarded; and,

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

**JURY TRIAL DEMANDED**

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: January 19, 2022

Respectfully Submitted,

*/s/ Terence R. Coates*
Terence R. Coates (0085579)
**MARKOVITS, STOCK & DEMARCO, LLC**
3825 Edwards Road, Suite 650

Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
*tcoates@msdlegal.com*

Joseph M. Lyon (0076050)
**THE LYON FIRM, LLC**
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
*jlyon@thelyonfirm.com*

*Attorneys for Plaintiff and the Proposed Class*