E-FILED
5/24/2024 3:57 PM
CLERK & MASTER
DAVIDSON CO. CHANCERY CT.

IN THE CHANCERY COURT FOR THE TWENTIETH JUDICIAL DISTRICT
DAVIDSON COUNTY, TENNESSEE

YVONNE PRATT, individually, and on behalf of all others similarly situated, **Plaintiff,** **v.** **SAINT THOMAS HEALTH D/B/A ASCENSION SAINT THOMAS** **Defendant.**	Case No. _____

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff, YVONNE PRATT, individually, and on behalf of all others similarly situated (hereinafter, "Plaintiff"), brings this Class Action Complaint, against Defendant SAINT THOMAS HEALTH D/B/A ASCENSION SAINT THOMAS ("Ascension" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, members, and/or other related entities, and upon personal knowledge as to her own actions, and information and belief as to all other matters, alleges as follows:

INTRODUCTION

1. This action arises out of the public exposure of the confidential, private information of Ascension's current and former patients—Plaintiff and the proposed Class Members—on or about May 8, 2024 during a cyberattack, caused by Defendant's failures to adequately safeguard that information ("the Data Breach"). On information and belief the information impacted in the Data Breach includes Personally Identifying Information[1] ("PII") and Protected Health

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government

Information ("PHI")[2] (collectively "Private Information").[3]

2. Headquartered in Nashville, Tennessee, Ascension is a massive healthcare system which holds itself out as "…one of the nation's leading non-profit and Catholic health systems, with a Mission of delivering compassionate, personalized care to all with special attention to persons living in poverty and those most vulnerable."[4]

3. As a condition of receiving treatment from Ascension, Defendant required its patients to provide it with their sensitive Private Information, which Ascension promised to protect from unauthorized disclosure.

4. Defendant failed to undertake adequate measures to safeguard the Private Information of Plaintiff and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

5. As a direct and proximate result of Defendant's failures to protect current and

---

passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the Data Breach.

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). Ascension is clearly a "covered entity" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

[3] *See Cybersecurity Event Update,* avail. at https://about.ascension.org/cybersecurity-event (last accessed May 15, 2024), **attached as Exhibit A.**

[4] https://about.ascension.org/about-us (last acc. May 15, 2024).

former patients' sensitive Private Information and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class Members have suffered widespread injury and damages, including interruption of care, necessitating Plaintiff to seek relief on a class wide basis.

PARTIES

6. Plaintiff is a natural person and resident and citizen of the State of Tennessee, where she intends to remain, who resides in Nashville, Tennessee in Davidson County. Plaintiff is a patient of Ascension and Data Breach victim.

7. Ascension is a not-for-profit corporation organized and existing under the laws of the State of Tennessee with a principal place of business at 102 Woodmont Boulevard, Suite 800 Nashville, Tennessee 37205 in Davidson County.

8. Defendant's Registered Agent for Service of Process is Corporation Service Company, 2908 Poston Avenue, Nashville, Tennessee 37203-1312.

JURISDICTION & VENUE

9. This Court has general jurisdiction over this action under T.C.A. § 16-10-101.

10. This Court has personal jurisdiction over Defendant because it resides and operates in this state.

11. Venue is proper in this Court under T.C.A. § 20-4-101 because Ascension resides in Davidson County, and the cause of action arose in this County.

COMMON FACTUAL ALLEGATIONS

A. Defendant Fails to Safeguard Patients' Private Information

12. Defendant is a massive Catholic healthcare system which provides treatment to patients across the country under a "commit[ment] to delivering compassionate and personalized

care for all, especially those who need it most."[5]

13. According to Ascension, it has "approximately 134,000 associates, 35,000 affiliated providers and 140 hospitals, serving communities in 19 states and the District of Columbia."[6]

14. Ascension provides medical treatment in Tennessee at numerous hospitals including: Ascension Saint Thomas Hospital Midtown and Ascension Saint Thomas Hospital West in Nashville; at Ascension Saint Thomas Rutherford and Ascension Saint Thomas Rutherford Westlawn in Murfreesboro; at Ascension Saint Thomas Stones River in Woodbury; Ascension Saint Thomas Hickman Hospital in Centerville; as well as through numerous medical centers and other clinics such as Ascension Saint Thomas Medical Partners Nashville.[7]

15. At its hospitals, medical centers, and other clinics, Defendant provides myriad medical services including, *inter alia*: Emergency care; Family medicine; Surgery; AFib and heart rhythm disorder care; Anxiety disorders; Arthritis and autoimmune diseases; Home Health Care; Brain and spine care; Breast cancer care; Breast health; Breastfeeding support; Burn care; Cancer care; Cardiology; Cosmetic and plastic surgery; Dermatology; Ear, nose and throat care; Eating disorders; Endocrinology and diabetes care; Epilepsy and seizure care; Gastroenterology; Gastrointestinal and colorectal cancers; Genetic testing and counseling; Gynecological care and surgery; Head and neck cancer care from ENT specialists; Headache disorders; Health screenings; Heart failure treatment; Heart surgery; High-risk pregnancy; Hip pain care; Hyperbaric oxygen therapy; Infectious disease care; Inpatient rehabilitation; Intensive care for newborns; Internal medicine; Kidney health; Lab services; Lung and esophageal cancer care; Mammography; Medical

[5] https://about.ascension.org/about-us (last acc. May 15, 2024).
[6] *Id*. (last acc. May 15, 2024).
[7] https://healthcare.ascension.org/find-care/search-result (last acc. May 15, 2024).

Oncology – Chemotherapy; Memory care and neuropsychology; Midwife care; Mood disorders and depression; Movement Disorders and Exercise for Balance Problems; Multiple sclerosis care; Neurology rehabilitation; Neurosurgery; Obstetrics and gynecology; Occupational Therapy; Oncology rehabilitation; Ophthalmology; Orthopedics; Pain Management; Palliative care; Pediatrics including surgery; Physical therapy; Podiatry; Pregnancy and birthing; Primary care; Prostate and male genital cancer care; Pulmonology - respiratory health; Radiation oncology; Radiology; Rehabilitation; Senior health care; Skin cancer care; Sleep disorder care; Spiritual care; Sports medicine and sports performance; Sports nutrition; Stroke care; Structural heart and valve care; Substance use and addiction disorders; Surgical Oncology; Trauma care; Urogynecology; Urology; Vascular surgery; Weight management and bariatric surgery; Women's health; and Wound care.[8]

16. On information and belief, Defendant generated approximately $241 million in revenue in 2022.[9]

17. As a condition of rendering medical treatment, Ascension requires that its patients provide Defendant with massive amounts of their Private Information, including, on information and belief, their names, dates of birth, Social Security Numbers, medical information such as diagnoses and treatment history, health insurance information, and payment information.

18. Ascension collects and stores this Private Information on its information technology computer systems, on information and belief located at its headquarters in Nashville, Tennessee.

[8] https://healthcare.ascension.org/specialty-care (last acc. May 15, 2024).
[9] https://projects.propublica.org/nonprofits/organizations/581716804 (last acc. May 15, 2024).

19. Defendant acknowledges the importance of protecting and securing the Private Information/PHI it collects, maintaining privacy policies including a Notice of Privacy Practices, which applies to "…all employees (associates), medical staff, trainees, students, volunteers, contractors, vendors, agents, and workforce members of Ascension Saint Thomas. Ascension Saint Thomas includes all Ascension hospitals, ambulatory care centers, pharmacies, laboratories, physician practices, and other Ascension health care providers located in Tennessee."[10]

20. Therein Ascension states that, "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."[11]

21. In the Notice of Privacy Practices, Defendant acknowledges and promises that:

- We are required by law to maintain the privacy and security of your health information.
- We will notify you if a breach occurs that may have compromised the privacy or security of your identifiable health information.
- We must follow the practices described in this Notice and provide you a copy of it.

22. Further, therein, Ascension represents and promises that it "…will not use or share your information other than as described here unless you tell us we can in writing..."[12]

23. In addition, in the Notice of Privacy practices, Ascension enumerates certain purposes for which it may disclose health information (PHI/Private Information) without authorization, *to wit*: for "treatment, payment, and health care operations purposes[;]" to notify patients about treatment alternatives, research opportunities, or other services, and for fundraising;

[10] *Ascension Saint Thomas Joint Notice of Privacy Practices,* eff. Jan. 1, 2023, avail. at https://healthcare.ascension.org/-/media/healthcare/npp/tennessee/tn_ascension-saint-thomas_english.pdf (last acc. May 15, 2024), **attached as Exhibit B.**
[11] *Id*.
[12] *Id*.

and for:

- Public health and safety: reporting communicable diseases, births, or deaths; reporting abuse, neglect, or domestic violence; reporting adverse reactions to medications; avoiding a serious threat to health or safety
- Law enforcement: to identify or find a suspect, fugitive, or missing person; to report a crime at the facility
- Judicial and administrative proceedings: responding to a court or administrative order, such as a subpoena
- Workers' compensation and other government requests: workers' compensation claims or hearings; health oversight agencies for activities authorized by law; special government functions (military, national security)
- Disaster relief: sharing your location and general condition for the purpose of notifying your family or friends and agencies chartered by law to assist in emergency situations
- Comply with the law: to the Department of Health and Human Services to see if we are complying with the federal privacy law
- Research: preparing for a research study; analyzing records as part of a project approved by an Institutional Review Board (IRB) and are low risk to your privacy; studies involving only decedents' information
- Incidental to a permitted use or disclosure: calling your name in a waiting area for an appointment and others may hear your name called. We make reasonable efforts to limit these incidental uses or disclosures.
- To a funeral director, coroner, or medical examiner as needed to do their jobs
- To organizations that handle organ, tissue, or eye donations and transplantations as needed to do their jobs.[13]

24. In addition, as stated in the Notice of Privacy Practices, Ascension may also disclose health information in health information exchanges (HIE) where other HIE participants must also protect health information; to family, friends, and other involved in care or payment for care; and in "a facility directory and chaplaincy services."[14]

25. None of the permitted purposes for Ascension's disclosure of patient health information, PHI/Private Information in Defendant's Notice of Privacy Practices the Data Breach.

[13] *Id*.
[14] *Id*.

26. Moreover, Defendant explicitly states in the Notice of Privacy Practices that:

> In the following situations, we will only use or share your health information if you give us written permission. You can take back this permission at any time (except to the extent that we have relied on it) by contacting the Privacy Officer.
>
> - for marketing purposes (as defined by the HIPAA Rules).
> - for the sale of your information or for payments from third parties.
> - certain sharing of psychotherapy notes.
> - **any other reasons not described in this Notice.**[15]

27. In addition, Ascension represented to its patients that it will undertake adequate measures to safeguard their Private Information.

28. Despite this, Defendant does not adequately safeguard patient health information, and does not follow industry standard practices in securing this data.

29. On or about May 8, 2024, Defendant suffered a ransomware cyberattack—the Data Breach. According to Ascension, as it posted to its website on May 9th in the *Cybersecurity Event Update*:

> On Wednesday, May 8, we detected unusual activity on select technology network systems, which we now believe is due to a cybersecurity event. At this time we continue to investigate the situation. We responded immediately, initiated our investigation and activated our remediation efforts. Access to some systems have been interrupted as this process continues.[16]

30. In the May 9, 2024 website notice, Defendant further stated that they had "initiated procedures to ensure patient care delivery continues to be safe and as minimally impacted as possible [but that] [t]here has been a disruption to clinical operations, and [it] continue[s] to assess the impact and duration of the disruption[;]" that it had partnered with a third party expert, Mandiant, to investigate and remediate the breach; and that it had notified unnamed "appropriate authorities."[17]

---

[15] *Id*. (bold emphasis added)
[16] *Cybersecurity Event Update,* **Exhibit A.**
[17] *Id*.

31. Later in the day on May 9th, Defendant updated its post, stating that the Data Breach had rendered unavailable "our electronic health records system, MyChart (which enables patients to view their medical records and communicate with their providers), some phone systems, and various systems utilized to order certain tests, procedures and medications" and that "[o]ut of an abundance of caution, however, some non-emergent elective procedures, tests and appointments have been temporarily paused while we work to bring systems back online."[18]

32. Further still, the Data Breach caused some of Ascension's hospitals to be put "on diversion for emergency medical services in order to ensure emergency cases are triaged immediately."[19]

33. In the following days, Defendant would provide periodic updates to its notice on its website. On May 11th, Ascension reported that the Data Breach was a ransomware attack, and that it had "notified law enforcement, as well as government partners including the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (HHS), and the American Hospital Association (AHA) […and is] sharing relevant threat intelligence with the Health Information Sharing and Analysis Center (H-ISAC)."[20]

34. Ultimately, in its Cybersecurity Event Updates, Defendant would neither confirm nor deny that patient's Private Information was impacted in the Data Breach, but that the investigation is ongoing and it will "notify and support" any individuals whose "sensitive information was affected." [21]

35. Despite the foregoing, Ascension have obfuscated key details of the Data Breach, failing to disclose to affected patients whether or not their information was unauthorizedly

[18] *Id*.
[19] *Id*.
[20] *Id*.
[21] *Id*., Patient—Frequently Asked Questions.

disclosed in the Data Breach; the identity of the ransomware cybercriminal; whether Defendant paid the ransom; whether the cybercriminals themselves have said that Ascension's Private Information was taken; and other pertinent details necessary for affected patients to take appropriate measures to protect themselves from the Data Breach.

36. On information and belief, Plaintiff's and the proposed Class Members' Private Information was unauthorizedly disclosed to third-party cybercriminals in Defendant's Data Breach on or about May 8, 2024, potentially including but not limited to their names, dates of birth, Social Security Numbers, medical information such as diagnoses and treatment history, health insurance information, and payment information.

37. In fact, this fact seems known to Ascension but not yet communicated by Defendant to its affected patients. According to media outlets, "[t]he healthcare network suspects the cyber attack possibly resulted in data exfiltration."[22]

38. Defendant's conduct, by acts of commission or omission, caused the Data Breach, including: Ascension's failures to implement best practices and comply with industry standards concerning computer system security to adequately safeguard Private Information, allowing Private Information to be accessed and stolen, by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach, and by failing to adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems, resulting in the Data Breach.

39. On information and belief, based on the nature of the ransomware cyberattack, Plaintiff and the members of the proposed Class Members' Private Information, unauthorizedly

[22] CPO Magaine, Alicia Hope, *Ascension Healthcare Network Cyber Attack Disrupts Operations Across Numerous Hospitals Across the US,* May 14, 2024, avail. at https://www.cpomagazine.com/cyber-security/ascension-healthcare-network-cyber-attack-disrupts-operations-across-numerous-hospitals-across-the-us/ (last acc. May 15, 2024).

disclosed to third-party cybercriminals in the Data Breach, has now or will imminently be posted to the Dark Web for public viewing and use, in the public domain, and utilized for fraudulent and criminal misuse.

B. Plaintiff's Experience

40. Plaintiff has been a patient of Ascension for many years, having received treatment at Ascension Saint Thomas Midtown in Nashville, Tennessee.

41. As a condition of receiving medical treatment from Defendant, Plaintiff was required to provide her Private Information to Ascension, including but not limited to her name, date of birth, Social Security Number, medical information such as diagnoses and treatment history, health insurance information, and payment information.

42. Plaintiff is very careful to guard the confidentiality of her Private Information, and never stores this information in an unsecure setting nor disseminates it publicly.

43. In entrusting her Private Information to Defendant as a condition of receiving medical care from Ascension, Plaintiff believed that Ascension would adequately safeguard that information, including as set forth in its Notice of Privacy Practices. Had Plaintiff known that Ascension did not utilize reasonable data security measures, Plaintiff would not have entrusted her Private Information to Defendant.

44. On information and belief Plaintiff's Private Information was unauthorizedly disclosed to third-party cybercriminals in Defendant's Data Breach on or about May 8, 2024 caused by Ascension's conduct.

45. As a direct and proximate result of the Data Breach permitted to occur by Defendant, Plaintiff has suffered, and imminently will suffer, injury-in-fact and damages, including the unauthorized disclosure of the Private Information itself, which, on information and

belief due to the nature of the cyberattack, has been or imminently will be posted on the dark web for sale and used for fraudulent and criminal purposes.

46. Moreover, the Data Breach, and Ascension's post-breach response, have seriously affected Plaintiff's ability to receive necessary emergency medical care and treatment, as on May 10, 2024 Plaintiff went to Ascension Saint Thomas Midtown Emergency Room due to an intestinal infection, but was turned her away due to the cyberattack and her medical records being unavailable, and was forced to go to TriStar Centennial hospital.

47. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of her Private Information in the Data Breach, and the lack of knowledge as to what information was disclosed.

48. In addition, as a result of the Data Breach Plaintiff has been and will be forced to expend considerable time and effort to monitor her accounts and credit files to protect herself from identity theft and fraudulent misuse of her Private Information disclosed in the Data Breach.

49. Had Plaintiff known that Defendant did not adequately protect her Private Information, she would not have entrusted her sensitive Private Information to Ascension.

50. Plaintiff's sensitive Private Information remains in Defendant's possession in its computer systems without adequate protection against known threats, exposing Plaintiff to future breaches and additional harm.

51. As a result of Ascension's Data Breach, its victims face too a lifetime risk of identity theft, and increased risk of harm.

C. This Data Breach was Foreseeable by Defendant.

52. Plaintiff and the proposed Class Members provided their Private Information to Ascension for the purpose of receiving medical treatment and with the reasonable expectation and

mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

53. By failing to do so, Defendant put all Class Members at risk of identity theft, financial fraud, and other harms.

54. Defendant tortiously failed to take the necessary precautions required to safeguard and protect the Private Information of Plaintiff and the Class Members from unauthorized disclosure. Defendant's actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights.

55. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that information.

56. According to a Chief Strategy Officer at Clear DATA, "[i]t's no secret that healthcare is the industry most plagued by data breaches. Patient data is the most valuable, making it targeted by bad actors."[23]

57. Moreover, healthcare companies are targeted because of their cybersecurity vulnerabilities: "…healthcare is also targeted because it is very vulnerable. Many healthcare providers use outdated IT infrastructure and operating systems that can no longer be patched or supported, such as Windows 7 and Windows Server 2008, even after Microsoft retired them. Further, more than half of medical devices operate on legacy systems, and 83% of medical imaging devices are on outdated operating systems that no longer receive patches/updates. This

[23] Sanjay Cherian, Forbes Magazine, "Healthcare Data: The Perfect Storm," January 14, 2022, available at https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=28523ee56c88 (last acc. June 19, 2023).

creates significant cybersecurity vulnerabilities and makes it much easier for bad actors to find an entry point into the network." [24]

58. Cyber-attacks against healthcare organizations, such Defendant, are targeted and frequent. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors…"[25]

59. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[26]

60. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[27]

61. According to the Identity Theft Resource Center's January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[28]

62. The increase in such attacks, and attendant risk of future attacks, was widely known

---

[24] *Id*.
[25] HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, *2019 HIMSS Cybersecurity Survey*, available at https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last accessed December 7, 2022)
[26] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 7, 2022)
[27] *Ibid.*
[28] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last acc. Apr. 14, 2023).

to the public and to anyone in Defendant's industry, including Ascension. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[29]

63. Furthermore, Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years. For instance, the 525 reported medical or healthcare data breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[30]

64. According to the U.S. Department for Health and Human Services' "2022 Healthcare Cybersecurity Year in Review, and a 2023 Look-Ahead," "[h]ealthcare data breaches have doubled in 3 years."[31]

65. 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 Ascension.

66. Private Information is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web,

67. Private Information can be used to distinguish, identify, or trace an individual's identity, such as their names, Social Security numbers, and medical records. This can be accomplished alone, or in combination with other personal or identifying information that is

[29] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last acc. Apr. 14, 2023).
[30] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 7, 2022), at pg. 15.
[31] U.S. Department for Health and Human Services, The Health Sector Cybersecurity Coordination Center (HC3), "2022 Healthcare Cybersecurity Year in Review, and a 2023 Look-Ahead," February 9, 2023, avail. at https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf

connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

68. Given the nature of the Data Breach, it was foreseeable that the compromised Private Information could be used by cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess the Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in their names.

D. Defendant Fails to Comply with Industry Standards

69. As shown above, experts studying cyber security routinely identify organizations holding PII/PHI as being particularly vulnerable to cyber-attacks because of the value of the information they collect and maintain.

70. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[32]

71. In addition, the National Institute of Standards and Technology (NIST)

[32] *See* https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Apr. 14, 2023).

recommends certain practices to safeguard systems, *infra,* such as:

a. Controlling who logs on to your network and uses your computers and other devices;

b. Using security software to protect data;

c. Encrypting sensitive data, at rest and in transit;

d. Conducting regular backups of data;

e. Updating security software regularly, automating those updates if possible;

f. Having formal policies for safely disposing of electronic files and old devices;

g. Training everyone who uses your computers, devices, and network about cybersecurity.[33]

72. Upon information and belief, Ascension failed to meet the minimum standards of both 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 established frameworks for reasonable cybersecurity readiness, and other industry standards for protecting Plaintiff's and the proposed Class Members' Private Information, resulting in the Data Breach.

E. Defendant Failed to Comply with FTC Guidelines

73. 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-

[33] Understanding The NIST Cybersecurity Framework, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Apr. 14, 2023).

making.

74. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of Private 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. 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.[34]

75. 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.[35]

76. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer 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.

---

[34] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).
[35] *See id*.

77. These FTC enforcement actions include actions against entities failing to safeguard PII/PHI such as 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.").

78. Defendant failed to properly implement basic data security practices widely known throughout the industry. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

79. Defendant was at all times fully aware of its obligations to protect the Private Information of Ascension's patients that was entrusted to Ascension. Defendant was also aware of the significant repercussions that would result from their failure to do so.

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

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

81. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of sensitive patient health information. Safeguards must include physical, technical, and administrative components.

82. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. § 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information, like the data Defendant left unguarded. 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).

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

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

a. Failing to adequately protect patients' Private Information;

b. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

c. Failing to practice the principle of least-privilege and maintain credential hygiene;

d. Failing to avoid the use of domain-wide, admin-level service accounts;

e. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords;

f. Failing to ensure the confidentiality and integrity of electronic PHI/ Private Information 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/ Private Information 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 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);

i. 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);

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

k. Failing to render the electronic PHI/ Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI/ Private Information 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);

85. As a result of its violations, Defendant negligently and unlawfully failed to safeguard Plaintiff's and the Class Members' Private Information.

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

86. Cyberattacks in the healthcare industry are especially problematic because of the disruption they cause to the health treatment and overall daily lives of patients affected by the attack.

87. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment due to a disruption of service.

88. This is exactly what happened in this case, with the Data Breach that Ascension permitted to occur not only making unavailable Ascension's electronic health records system, MyChart, telephone systems, and "various systems utilized to order certain tests, procedures and medications" but actually preventing the Plaintiff and Class Members from accessing Defendant's medical care.

89. Such disruptions lead to a deterioration in the quality of overall care patients receive at facilities affected by data breaches. This is an especially acute problem, because it is not as if incarcerated Class Members have any choice in who provides them care.

90. Researchers have found medical facilities that experience a data security incident incur an increase in the death rate among patients months and years after the attack.[36]

91. Researchers have further found that at medical facilities that experience a data security incident, the incident leads to a deterioration in patient outcomes, generally.[37]

92. Similarly, data security incidents inconvenience patients; these inconveniences include, but are not limited, to the following:

a. rescheduling of medical treatment;

b. being forced to find alternative medical care and treatment;

c. delays or outright cancellation of medical care and treatment;

d. undergoing medical care and treatment without medical providers having

[36] *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 (last accessed June 7, 2022).

[37] *See Data Breach Remediation Efforts and Their Implications for Hospital Quality*, Health Services Research https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last accessed June 7, 2022).

access to a complete medical history and records; and

e. the indefinite loss of personal medical history.[38]

93. Cyber-attacks that result in the removal of protected data are also considered a breach under HIPAA as there is an access of PHI not permitted under the HIPAA Privacy Rule:

94. 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." 45 C.F.R. § 164.40.

95. Data Breaches like this represent a significant problem for patients who have already experienced the inconvenience and disruption associated with a cyber-attack.

H. The Data Breach Caused Plaintiff and the Class Members Injury and Damages

96. Plaintiff and members of the proposed Class have suffered injury and damages from the unauthorized disclosure and misuse of their Private Information that can be directly traced to Defendant, that has occurred, is ongoing, and/or will imminently occur.

97. As stated prior, on information and belief, in the Data Breach, unauthorized cybercriminals were able to access the Plaintiff's and the proposed Class Members' Private Information, which is now being used or will imminently be used for fraudulent purposes and/or has been sold for such purposes and posted on the Dark Web for sale, causing widespread injury and damages.

98. The ramifications of Defendant's failure to keep Plaintiff's and the Class's Private Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's

[38] *See, e.g.*, https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/ (last accessed September 1, 2021); https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech (last accessed on September 1, 2021).

license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

99. Because Defendant failed to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer injury-in-fact and damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the Class Members have suffered, and will imminently suffer:

a. Disruption of medical care;

b. The loss of the opportunity to control how Private Information is used;

c. Unauthorized use of stolen Private Information;

d. Emotional distress;

e. The compromise and continuing publication of their Private Information;

f. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

g. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

h. The diminution in value of their Private Information;

i. Delay in receipt of tax refund monies; and,

j. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Ascension fails to undertake the appropriate measures to protect the Private

Information in its possession.

100. Furthermore, the Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft.

101. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[39]

102. The FTC recommends that identity theft victims take several costly 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, seeking a credit freeze, and correcting their credit reports.[40]

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

---

[39] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last acc. Feb. 27, 2023).

[40] *See* https://www.identitytheft.gov/Steps (last visited September 1, 2021).

104. 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.

105. 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 Private Information to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

106. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: "For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. Thirty-three percent reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. Fifty-four percent reported feelings of being violated." [41]

107. What's more, theft of PHI is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, Private Information/PHI is a valuable property right.[42]

---

[41] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last acc. Feb. 27, 2023).

[42] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private information") Equals the "Value" of Financial Assets*, 15

108. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that Private Information has considerable market value.

109. Theft of PHI, in particular, is problematic because: "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."[43]

110. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII/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.

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

112. PHI and PII are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

113. Where the most Private Information belonging to Plaintiff and Class Members was

---

Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private information, 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).

[43] *See Medical Identity Theft, Federal Trade Commission Consumer Information* (last visited: June 7, 2022), http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

accessible from Defendant's network, 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 the Class Members are at an increased risk of fraud and identity theft for many years into the future.

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

115. According to cybersecurity experts, "[r]eports show the value of a health record can be worth as much as $1,000, whereas on the dark web, a credit card number is worth $5 and Social Security numbers are worth $1."[44]

116. Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[45]

117. 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. 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.[46] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number

[44] Sanjay Cherian, Forbes Magazine, "Healthcare Data: The Perfect Storm," January 14, 2022, available at https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=28523ee56c88 (last acc. June 19, 2023).
[45] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last acc. Feb. 25, 2023)
[46] *See id.*

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.

118. Moreover, it is not an easy task to change or cancel a stolen Social Security number. 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."[47]

119. 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."[48] Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is $50 per person and up.[49]

120. Accordingly, the Data Breach has caused Plaintiff and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the imminent identity fraud and criminal fraudulent activity, fraudulent charges, theft of monies, and attendant costs; lost time and efforts in remediating the impact of the Data Breach, and other injury and damages as set forth in the preceding paragraphs.

---

[47] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 1, 2021).

[48] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited September 1, 2021).

[49] *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 accessed September 1, 2021).

121. Defendant knew or should have known of these harms which would be caused by the Data Breach it permitted to occur, and strengthened its data systems accordingly.

CLASS ACTION ALLEGATIONS

122. Plaintiff sues on behalf of herself and the proposed Class, defined as follows:

> **All Tennessee citizens whose Private Information was disclosed, accessed, or compromised in the Data Breach experienced by Ascension beginning on or about May 8, 2023, as announced by Defendant.**

123. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's members, partners, subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parents has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

124. The Class defined above is identifiable through Defendant's business records.

125. Plaintiff reserves the right to amend the class definition.

126. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Tenn. R. Civ. P. 23.01(1)-(4):

a. Numerosity. Plaintiff is representative of the proposed Class, consisting of potentially thousands or even millions of individuals, which are identifiable based on Defendant's records, and far too many to join in a single action;

b. Typicality. Plaintiff's claims are typical of Class Member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same

unreasonable manner of notifying individuals about the Data Breach.

c. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's interests. Plaintiff's interests do not conflict with Class Members' interests and Plaintiff has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel. Defendant has no defenses unique to Plaintiff.

d. Commonality. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Common questions for the Class include, but are not necessarily limited to the following:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Private Information;

ii. 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;

iii. Whether Ascension was negligent in maintaining, protecting, and securing Private Information;

iv. Whether Defendant breached contractual promises to safeguard Plaintiff's and the Class's Private Information;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Data Breach notice was reasonable;

vii. Whether Defendant's conduct was likely to deceive the public;

viii. Whether Defendant is liable for negligence;

ix. Whether Defendant was negligent *per se*;

x. Whether Defendant's practices and representations related to the Data Breach breached implied contracts;

xi. Whether Defendant was unjustly enriched;

xii. Whether the Data Breach caused Plaintiff and the Class injuries and damages;

xiii. What the proper damages measure is; and

xiv. Whether Plaintiff and the Class are entitled to damages, or declaratory and injunctive relief.

127. Further, this action satisfies Tenn. R. Civ. P. 23.02 because: (i) common questions of law and fact predominate over any individualized questions; (ii) prosecuting individual actions would create a risk of inconsistent or varying adjudications, risking incompatible standards of conduct for Defendant, and a risk adjudications with respect to individual Class Members which would as a practical matter be dispositive of the interests of the other members not parties to the adjudications or would substantially impair or impede their ability to protect their interest; and (iii) the Defendant have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

128. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

129. Plaintiff and the Class Members entrusted their Private Information to Ascension as a condition of receiving.

130. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using the Private Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

131. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure to collectively adequately safeguard their Private Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Private Information—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members's Private Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

132. Defendant owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their Private Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

133. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew

or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Class Members's Private Information as a condition of providing medical treatment to them.

134. The risk that unauthorized persons would attempt to gain access to the Private Information, and misuse it, was foreseeable. Given that Defendant holds vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information—whether by a sophisticated ransomware cyberattack or otherwise.

135. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

136. Defendant breached its duties by failing to exercise reasonable care in supervising its agents and in handling and securing the Private Information of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff's and Class Members' injuries, and is negligent.

137. Defendant is further breaching its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Class Members' injuries-in-fact.

138. As a direct, proximate, and traceable result of Defendant's negligence, Plaintiff and the Class Members have suffered or will imminently suffer injury-in-fact and damages, including but not limited to disruption of medical care; loss of the opportunity to control how Private Information is used; unauthorized use of stolen Private Information; emotional distress;

compromise and continuing publication of their Private Information; Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; diminution in value of their Private Information; Delay in receipt of tax refund monies; and, the continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Ascension fails to undertake the appropriate measures to protect the Private Information in its possession.

139. As a direct and proximate result, Plaintiff and the Class are entitled to recover damages including actual and compensatory damages, nominal damages, and punitive damages, as permitted by law.

140. Further, Plaintiff and the Class are entitled to injunctive relief ordering Defendant to strengthen its data security systems, monitoring procedures, and data breach notification procedures to prevent additional unauthorized disclosure of the Private Information in Defendant's possession.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

141. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

142. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

143. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' Private Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive Private Information.

144. Further, under HIPAA, Defendant had the duty to implement safeguards to prevent the misuse of the information and ensure the confidentiality, integrity, and availability of PHI/Private Information.

145. Defendant violated its duties under Section 5 of the FTC Act, as well as HIPAA, by failing to use reasonable measures to protect Plaintiff's and the Class's Private Information and by not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Ascension had collected, and stored, and the foreseeable consequences of a Data Breach, including, specifically, the immense damages that would result to its patients in the event of a breach, which ultimately came to pass.

146. The harm that has occurred is the type of harm the FTC Act and HIPAA are intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

147. Defendant had a duty to Plaintiff and the Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's Private Information.

148. Defendant breached its duties to Plaintiff and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information, and to supervise their vendors to ensure they did so.

149. Defendant's violations of Section 5 of the FTC Act and their failure to comply with applicable laws and regulations, including HIPAA, constitutes negligence *per se*.

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

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

152. Had Plaintiff and Class Members known that Defendant did not adequately protect their Private Information, Plaintiff and Class Members would not have entrusted Defendant with their Private Information.

153. As a direct, proximate, and traceable result of Defendant's negligence *per se*, Plaintiff and the Class Members have suffered or will imminently suffer injury-in-fact and damages, including but not limited to disruption of medical care; loss of the opportunity to control how Private Information is used; unauthorized use of stolen Private Information; emotional distress; compromise and continuing publication of their Private Information; Out-of-pocket

expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; diminution in value of their Private Information; Delay in receipt of tax refund monies; and, the continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Ascension fails to undertake the appropriate measures to protect the Private Information in its possession.

154. As a direct and proximate result, Plaintiff and the Class are entitled to recover damages including actual and compensatory damages, nominal damages, and punitive damages, as permitted by law.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

155. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

156. Defendant offered to provide medical service and data security to Plaintiff and the Class Members in exchange for payment and Private Information.

157. In turn, and through internal policies described in the preceding paragraphs, and other conduct and representations, Ascension agreed it would not disclose the Private Information it collects to unauthorized persons and that it would safeguard patient Private Information.

158. Plaintiff and the Class Members accepted Ascension's offer by providing Private Information to Defendant and paying money for medical treatment.

159. Implicit in the parties' agreement was that Ascension would adequately safeguard the Private Information of Plaintiff and the Class Members and would provide them with prompt

and adequate notice of all unauthorized access and/or theft of their Private Information.

160. Plaintiff and the Class Members would not have entrusted their Private Information to Ascension in the absence of such an agreement with Defendant.

161. Ascension materially breached the contract(s) it had entered into with Plaintiff and the Class Members by failing to safeguard their Private Information, and by failing to notify them promptly of the Data Breach that compromised such information. Ascension further breached the implied contracts with Plaintiff and the Class Members by:

a. Failing to properly safeguard and protect Plaintiff's and Class Members's Private Information;

b. Failing to comply with industry standards, as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to properly supervise its agents in possession of Private information;

d. Failing to ensure the confidentiality and integrity of electronic Private Information that Defendant created, received, maintained, and transmitted.

162. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of Ascension's material breaches of its agreement(s).

163. Plaintiff and the Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Ascension.

164. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the

parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

165. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

166. Ascension failed to advise Plaintiff and Class Members of the Data Breach promptly and sufficiently.

167. In these and other ways, Ascension violated its duty of good faith and fair dealing.

168. Plaintiff and the Class Members have sustained injury-in-fact and damages because of Ascension's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

169. Plaintiff incorporates the above Paragraphs 1-158 if fully set forth herein.

170. This claim is pleaded as the alternative to the breach of implied contract claim.

171. Plaintiff and the Class Members conferred a benefit upon Defendant in the form of Private Information provided to Defendant, along with payment, as a condition of receiving medical care.

172. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class Members.

173. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the value of their labor with reasonable data privacy and security practices and procedures, and the value of labor without

unreasonable data privacy and security practices and procedures that they received.

174. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class Members' labor and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the Class Members would not have provided their Private Information, nor rendered labor to Defendant, had they known Defendant would not adequately protect their Private Information.

175. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach alleged herein.

COUNT V
INVASION OF PRIVACY—PUBLIC DISCLOSURE OF PRIVATE FACTS
(On Behalf of Plaintiff and the Class)

176. Plaintiff incorporates the above Paragraphs as if fully set forth herein.

177. The Plaintiff and the Class Members took reasonable and appropriate steps to keep their Private Information confidential from the public.

178. Plaintiff's and the Class Members' efforts to safeguard their own Private Information were successful, as their Private Information was not known to the general public prior to the Data Breach.

179. Plaintiff and the Class Members had a legitimate expectation of privacy to their Private Information, entrusted solely to Ascension for purpose of receiving medical care, and were entitled to the protection of this information against disclosure to unauthorized third parties.

180. Defendant owed a duty to Ascension's patients, including Plaintiff and the Class Members, to keep their Private Information confidential.

181. The unauthorized release of Private Information by Defendant in the Data Breach

is highly offensive to a reasonable person.

182. Plaintiff's and the Class Members' Private Information is not of legitimate concern to the public.

183. Defendant knew or should have known that Plaintiff's and Class Members' Private Information was private, confidential, and should not be disclosed.

184. Defendant publicized Plaintiff's and Class Members's Private Information, by unauthorizedly disclosing it to cybercriminals who had no legitimate interest in this Private Information and who had the express purpose of monetizing that information through fraudulent misuse and by injecting it into the illicit stream of commerce flowing through the Dark Web.

185. Indeed, not only was Plaintiff's and Class Members's Private Information exfiltrated from Ascension's systems, but, upon information and belief, has been or will imminently be published on the Dark Web and used to commit fraud; and is being disseminated amongst, *inter alia,* other criminals, financial institutions, merchants, creditors, health care providers and governmental agencies.

186. It is therefore substantially certain that the Plaintiff's and the Class Members' Private Information is rapidly becoming public knowledge—among the community at large—due to the nature of the cyber-attack that procured it, and the identity theft for which it is designed.

187. As a direct and proximate result of the invasion of privacy, public disclosure of private facts committed by Defendant, Plaintiff and the Class Members have suffered injury-in-fact and damages as set forth in the preceding paragraphs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, YVONNE PRATT, individually, and on behalf of all others similarly situated, requests that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

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

Dated: May 24, 2024

Respectfully submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV (No. 23045)

Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Lynn A. Toops*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
Telephone: (317) 636-6481
ltoops@cohenandmalad.com

*_Pro Hac Vice_ forthcoming

Counsel for Plaintiff and the Proposed Class