IN THE CIRCUIT COURT OF THE CITY OF ST. LOUIS
STATE OF MISSOURI

JOHN DOE and JANE DOE, individually and on behalf of all others similarly situated,	
Plaintiffs,	**CASE NO. _____**
VS.	
SSM HEALTH CARE CORPORATION D/B/A SSM HEALTH SERVE AT: C T Corporation System, Registered Agent 120 South Central Avenue Clayton, Missouri 63105	**JURY TRIAL DEMANDED**
and	
NAVVIS & COMPANY, LLC SERVE AT: Adam Schneider, Registered Agent 555 Maryville University Drive, Suite 240 St. Louis, Missouri 63141,	
Defendants.	

CLASS ACTION PETITION

Plaintiffs JOHN DOE and JANE DOE ("Plaintiffs") bring this action on behalf of themselves, and all others similarly situated, against Defendants, SSM HEALTH CARE CORPORATION D/B/A SSM HEALTH ("SSM") and NAVVIS & COMPANY, LLC ("Navvis") (collectively "Defendants"), and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

NATURE OF THE ACTION

1. This action arises out of Defendants' failures to adequately protect the confidential

medical information, Personally Identifying Information[1] ("PII") and Protected Health Information ("PHI")[2] (collectively, "Private Information") of SSM's current and former patients, including Plaintiffs and the proposed Class Members, resulting in the unauthorized disclosure of that Private Information between July 12, 2023 and July 25, 2023 during a cyberattack to Navvis' systems, including their names, dates of birth, Medicaid/Medicare ID numbers, health plan information, medical treatment information, medical record numbers, patient account numbers, case identification numbers, provider and doctor information and health record information, and Social Security numbers (the "Data Breach").[3]

2. Headquartered in St. Louis, Missouri, SSM is a massive not-for-profit healthcare

---

[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 passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[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). SSM is a covered entity, and Navvis is a Business Associate, under HIPAA, and some of the data compromised in the Data Breach that this action arises out of is "protected health information," subject to HIPAA.

[3] *See* SSM Health, *Data security breach information,* available at https://www.ssmhealth.com/data-security-incidents-your-protected-health-information (last acc. Feb. 2, 2024) linking to Navvis *Notice of Data Event*, available at https://navvishealthcare.com/privacy-update (last acc. Feb. 2, 2024) **attached as Exhibit A;** Navvis, *Notice of Security Incident to John Doe***,** December 29, 2023, **attached as Exhibit B;** and *Notice of Security Incident to Jane Doe*, December 29, 2023, **attached as Exhibit C.**

system which provides care and treatment to patients in Missouri, Illinois, Oklahoma, and Wisconsin.[4]

3. Navvis is a company located in St. Louis which provides health management services to SSM.[5]

4. As a condition of providing medical services, SSM requires its patients, including Plaintiffs and the Class Members, to provide it with their Private Information, which it provides to Navvis, and which Defendants each store in their computer network systems.

5. Defendants failed to undertake adequate measures to safeguard the Private Information of Plaintiffs and the proposed Class Members, including Navvis failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, and SSM failing to ensure Navvis undertook such measures, resulting in the Data Breach.

6. Although the Data Breach was discovered on or about July 25, 2023, Defendants failed to immediately notify and warn Data Breach victims of the unauthorized disclosure of their Private Information, waiting until December 2023 to notify impacted patients, Plaintiffs and the Class.

7. As a direct and proximate result of Defendants' failures to protect Plaintiffs' and the Class Members' sensitive Private Information and warn them promptly and fully about the Data Breach, Plaintiffs and the proposed Class have suffered widespread injury and damages necessitating Plaintiffs seeking relief on a class wide basis.

THE PARTIES

[4] https://www.ssmhealth.com/ (last acc. Feb. 2, 2024)
[5] SSM Health, *Data security breach information,* available at https://www.ssmhealth.com/data-security-incidents-your-protected-health-information (last acc. Feb. 2, 2024)

8. Plaintiff John Doe is a natural person and Missouri citizen, residing in St. Louis, Missouri, where he intends to remain. Plaintiff John Doe is a Data Breach victim who received Navvis' letter dated December 29, 2023 notifying him of the Data Breach.

9. Plaintiff Jane Doe is a natural person and Missouri citizen, residing in St. Louis, Missouri, where she intends to remain. Plaintiff Jane Doe is a Data Breach victim who received Navvis' letter dated December 29, 2023 notifying her of the Data Breach.

10. Defendant SSM HEALTH CARE CORPORATION d/b/a SSM Health ("SSM") is a corporation organized and existing under the laws of the State of Missouri, with a principal place of business located at 12800 Corporate Hill Drive, Saint Louis, Missouri 63131-1845.

11. SSM's Registered Agent for Service of Process is C T Corporation System, 120 South Central Avenue, Clayton, Missouri 63105.

12. Defendant NAVVIS & COMPANY, LLC ("Navvis") is a limited liability company organized and existing under the laws of the State of Delaware, with a principal place of business located at 555 Maryville University Drive, Suite 240, St. Louis, Missouri 63141.

13. Navvis' Registered Agent for Service of Process is Adam Schneider, 555 Maryville University Drive, Suite 240, St. Louis, Missouri 63141.

JURISDICTION AND VENUE

14. This court is vested with subject-matter jurisdiction pursuant to Mo. Stat. § 478.070.

15. This Court has personal jurisdiction over Defendants because they maintain principal places of business in Missouri, and each provide healthcare services in Missouri.

16. Venue is proper in this Court pursuant to MO Stat. § 508.010 because Plaintiffs were first injured by Defendants' acts or conduct in the City of St. Louis, Missouri and Defendants do business in the City of St. Louis, Missouri.

COMMON FACTUAL ALLEGATIONS

A. Defendants, SSM and Navvis

17. SSM holds itself out as a "large, multi-state health system that puts the care for our patients, their families and visitors first[,]"[6] a "…a Catholic, not-for-profit health system serving the comprehensive health needs of communities across the Midwest through a robust and fully integrated health care delivery system."[7]

18. SSM has "40,000 team members and more than 12,800 providers are committed to providing exceptional health care services and revealing God's healing presence to everyone they serve."[8]

19. SSM's system includes "23 hospitals, more than 300 physician offices and other outpatient and virtual care services, 12 post-acute facilities, comprehensive home care and hospice services, a pharmacy benefit company, a health insurance company and an accountable care organization."[9] Indeed, SSM has three hospitals in St. Louis—SSM Health Saint Louis University Hospital, SSM Health Cardinal Glennon Children's Hospital, and SSM Health St. Mary's Hospital - St. Louis.[10]

20. SSM reports having 163,411 inpatient admissions, 2 million outpatient visits, 5.7 million completed medical group appointments, 90,368 outpatient surgeries, nearly 23,000 monthly virtual visits, and 241,428 home care visits.[11]

21. At its many locations, SSM provides myriad medical services, including:

---

[6] https://www.ssmhealth.com/resources
[7] https://www.ssmhealth.com/resources/about
[8] *Id.*
[9] *Id*
[10] https://www.ssmhealth.com/location-results/Hospital?range=25&zip=63110&lat=38.633024&lng=-90.244086#locationResults
[11] https://www.ssmhealth.com/resources/about

Emergency Services, surgery, Addiction Treatment, Adjustable Gastric Band, Aesthetic Surgery, A-Fib Ablation, Allergies, Allergy & Immunology, Allergy Testing, Aneurysm, Angina, Angioplasty/Stenting Procedures, Ankle & Foot Pain, Anticoagulation Therapy Management, Aortic Insufficiency, Aortic Valve Stenosis, Arrhythmia & Atrial Fibrillation, Asthma Audiology Autonomic Function Testing AV Malformation, Baby Blues & Perinatal Mood & Anxiety Disorders (PMAD), Back Pain, Back Surgery, Bariatric Surgery, Bariatrics, Bed Wetting, Behavioral Health, Birthing, Bladder Cancer, Bladder Control, Blood & Bone Marrow Transplant, Blood Pressure, Body (Bariatric) Contouring, Bone & Soft Tissue Cancer, Bone Density Imaging, Bone Fractures, Botox, Brain & Spinal Cord Tumors, Brain Anatomy, Brain Injury, Brain Tumors, Breast Cancer, Breast Health, Breast Reconstruction, Breast Reduction, Breast Self Exams, Breast Surgery, Breastfeeding Support, Broken Bone, Bronchial Thermoplasty, Bronchoscopy, Cancer Care & Support, Cancer Surgery, CAR T-cell Therapy, Cardiac Cath Lab, Cardio/Pulmonary Rehabilitation, Cardiology, Carpal Tunnel Syndrome, Cervical Cancer, Cervical Spondylosis, Cesarean Section (C-Section), Chemical Dependency, Chest & Lung Health, Child Care Center, Childbirth Options, Children's Health, Chronic Care Management, Cold and Flu, Colon Cancer, Colonoscopy, Complex Spine Surgery, Concussions, Congestive Heart Failure, Coronary Artery Disease, Cosmetic Services, COVID-19 Testing, CT or Cat Scan, Cyberknife, Degenerative Disc Disease, Depression, Dermatology, DEXA Scan, Diabetes, Diabetes Self-Management Education, Domestic Violence Services, Duodenal Switch, EKG, Electrophysiology, Emergency Services, Endocrinology, Endometriosis, Endoscopic Retrograde Cholangiopancreatography (ERCP), Endoscopic Ultrasound, Enlarged Prostate, ENT, Enteral Therapy Management (Health at Home Wisconsin), Epilepsy, Esophageal Cancer, E-Visits, Express Virtual Care, Eye Care, Facial Cosmetic Surgery, Family Medicine, Fenestrated Endovascular Aortic Aneurysm Repair

(FEVAR), First Trimester Screening, Flexible Sigmoidoscopy, Foot & Ankle Orthopedics, Gastric Band, Gastric Bypass, Gastroenterology, Gastrointestinal Cancer, Genetic Counseling (Cancer), Genetic Testing (Pregnancy), Geriatrics, Gestational Diabetes, Glasses & Contacts, Glaucoma, Grief & Bereavement, Gynecology, Hand, Wrist & Elbow Orthopedics, Headache, Health at Home Specialty Services (Orthopedics & Parkinson's Program), Heart & Vascular Diagnostic Services, Heart Attack, Heart Care, Heart Disease & Women, Heart Murmur, Heart Valve Repair Surgery, Hematology, Hemorrhagic Stroke, Hepatitis C Virus, Herniated or Ruptured Discs, High Blood Pressure, High-Risk Pregnancy, Hill-Sachs Lesion, Hip & Knee, Hip Replacement Surgery, HIPEC, Home Health Services, Home Infusion Services (Health at Home Wisconsin), Hospice Services, Hyperbaric Chamber Treatment, Image-Guided Radiation Therapy, Imaging, Immunizations, Incontinence, Infectious Disease, Insomnia, Integrative Medicine, Internal Medicine, InterStim Therapy, Interventional Pulmonology, Interventional Radiology – Fibroids, Intragastric Balloons, Ischemic Stroke, Joint Replacement, Kidney Cancer, Kidney Dialysis, Kidney Stone Treatment, Kidney Transplant, Knee Replacement Surgery, Lactation Support, Language Assistance, LAP-BAND, Lead Extraction, Leadless Pacemaker, Leukemia, Ligament Injuries, Liver Cancer, Liver Disease, Liver Transplant, Living Donor Kidney Transplantation, Lung Cancer, Lymphedema Services, Mammogram Scheduling, Maternal Fetal Medicine Telemedicine, Maternity Care, Meals on Wheels (Health at Home Wisconsin), Mechanical Clot Removal, Medicare Wellness, Melanoma, Menopause, Men's Health, Mental Health, MidAmerica Stroke Network, Midwifery Care, Minimally Invasive Bypass, Minimally Invasive Maze, Minimally Invasive Spine Surgery, MitraClip, Mitral Insufficiency, Mitral Valve Replacement, Mitral Valve Stenosis, Mohs Procedure, Mouth & Throat Cancer, Movement Disorders, MRI, Multiple Myeloma, Multiple Sclerosis, Neonatal Care, Nephrology, Neurology Services,

Neuropsychology, Neurosciences, Neurosurgery Services, Non-Surgical Treatment for Heart Disease, Non-Surgical Weight Loss Options, Nutrition Services, Obesity, Obstetrics – OBGYN, Occupational Therapy, Oculoplastic Surgery, Oncology, Open Heart Surgery, Ophthalmology, Optometry, Orthopedics, Osteoporosis, Otolaryngology, Ovarian Cancer, Pain Care & Management, Palliative Care, Pancreas Transplant, Pancreatic Cancer, Parkinson's Disease, Pastoral Care, Pediatrics, Pelvic Health, Peripheral Artery Disease, PET Imaging, Pharmacotherapy, Pharmacy & Prescription Centers, Physical Therapy, Plastic Surgery, Podiatry, Pregnancy, Preventative Cardiology & Rehab, Preventing Heart & Cardiovascular Disease, Primary Care, Prostate Artery Embolization - Interventional Radiology, Prostate Cancer, Prostate Health, Psychiatric Care, Pulmonology, Radiation Therapy, Radiosurgery, Reconstructive Surgery, Refractive Eye Surgery, Revisional Weight Loss Surgery, Rheumatology, Robotic Heart Valve Surgery, Robotic-Assisted Surgery, Sciatica, Scoliosis, Senior Health, Shoulder & Upper Extremity, Skin Cancer, Skin Procedures, Sleep, Sleep Disorders, Sleeve Gastrectomy, Specialty Pharmacy, Speech Therapy, Spider Veins, Spinal Stenosis, Spine & Back, Spine Surgery, Spondylolisthesis, Sports Injuries, Sports Medicine, Sports Physicals, SSM Health at Home, Stroke, Stroke Centers, Stroke Rehabilitation, Stroke Telemedicine, Substance Abuse, Surgical Services, Telehealth, Tendonitis, Therapy & Rehabilitation, Thoracic Surgery, Thyroid Cancer, Tomo Therapy, Total Hip Replacement, Total Knee Replacement, Total Shoulder Replacement, tPA Stroke Treatment, Transcatheter Aortic Valve Replacement, Transplant Services, Trauma Reconstructive Plastic Surgery, Trauma Services, Traumatic Brain Injury, Travel Medicine, Trigeminal Neuralgia, Ultrasound, Urgent Care - Express Clinics, Urogynecology, Urological Cancer, Urology, Uterine Cancer, Valvular Disease, Vascular Services, Venous Disease, Veterans Care (Hospice), Virtual Care, VoiceCare (Health at Home Wisconsin), Vulvar Pain, Weight

Management, Weight Management Nutrition Support, Well-Woman Exam, Women's Health, Wound Care, and X-Rays.[12]

22. Navvis is a "Population Health, Value-Based Care Company" which provides health management services to SSM and other health care organizations.[13]

23. As a condition of providing medical services, SSM requires that its patients provide SSM with their valuable, Private Information—including their names, dates of birth, Medicaid/Medicare ID numbers, health plan information, medical treatment information, medical record numbers, patient account numbers, case identification numbers, provider and doctor information and health record information, and Social Security numbers—which SSM then provided to Navvis in connection with Navvis' health management services.

24. SSM understands the importance of safeguarding Private Information, including PHI, maintaining a Notice of Privacy Practices, which states:

> We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. We create a record of the health care services you receive from us. We need this record to provide you with quality health care services and to comply with certain legal requirements. This Notice applies to all of the records of your care that we generate.[14]

25. In its Notice of Privacy Practices, SSM acknowledges, represents and promises that it is required by law to: "• Make sure that medical information that identifies you is kept private;

---

[12] https://www.ssmhealth.com/services

[13] https://www.navvishealthcare.com/; *See* SSM Health, *Data security breach information,* available at https://www.ssmhealth.com/data-security-incidents-your-protected-health-information (last acc. Feb. 2, 2024) linking to Navvis *Notice of Data Event*, available at https://navvishealthcare.com/privacy-update (last acc. Feb. 2, 2024) **Exhibit A;** Navvis, *Notice of Security Incident to John Doe***, Exhibit B;** and *Notice of Security Incident to Jane Doe*, **Exhibit C.**

[14] SSM, *Notice of Privacy Practices*, effective June 30, 2018, available at https://www.ssmhealth.com/privacy-notices-terms-of-use/notice-privacy-practices (last acc. Feb. 2, 2024), attached as Exhibit D.

• Give you this Notice of our legal duties and privacy practices with respect to medical information about you; and • Follow the terms of the Notice that is currently in effect."[15]

26. Therein, SSM enumerates certain purposes for which it may disclose PHI without authorization, including for: treatment; payment; for health care operations; as part of its Organized Health Care Arrangement; for appointment reminders; to recommend treatment alternatives; for health-related benefits and services; for patient assistance programs; for fundraising activities; in a hospital directory; to individuals involved in patient care or payment for care; for research purposes; as required by law; and in special situations, such as in connection with organ and tissue donations; for members of the armed forced, to military command authorities; for worker's compensation claims; for public health activities; for health oversight activities; in lawsuits and disputes; to law enforcement; to coroners, medical examiners and funeral directors; for national security and intelligence activities; and for inmates, to correctional institutions.[16]

27. None of the foregoing purposes include the unauthorized disclosure of patients' PHI/Private Information as occurred in the Data Breach.

28. In addition, in its Notice of Privacy Practices, SSM states that "other uses and disclosures of medical information not covered by this Notice or the laws that apply to us will be made only with your written permission." [17]

29. Further, as stated in SSM's Notice of Privacy Practices, it states that patients "have the right to receive notifications of breaches of your unsecured medical information."[18]

30. In addition, SSM, by and through its agents and employees, represented to its

[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*

patients, that Defendants would adequately protect their Private Information and not disclose said information other than as authorized.

31. Plaintiffs and the proposed Class Members, current and former patients of Defendants, would not have entrusted their Private Information to SSM, and in turn to Navvis, in the absence of Defendants' promises to safeguard that information.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the proposed Class Members' Private Information, Defendants assumed legal and equitable duties to Plaintiffs, and the members of the Proposed Class, and knew or should have known that they were responsible for protecting their Private Information from unauthorized disclosure.

33. At all times Plaintiffs and the members of the Proposed Class, have taken reasonable steps to maintain the confidentiality of their Private Information; and, Plaintiffs and the proposed Class Members, as current and former patients of SSM, relied on SSM and Navvis to keep their Private Information confidential and securely maintained.

B. Defendants Fail to Adequately Safeguard Patients' Private Information—the Data Breach

34. Plaintiffs and the proposed Class Members are current and former patients of SSM, whose Private Information was provided by SSM to Navvis.

35. As a condition of providing medical treatment to its patients, SSM required Plaintiffs and the proposed Class Members to provide SSM with their sensitive, Private Information, including their names, dates of birth, Medicaid/Medicare ID numbers, health plan information, medical treatment information, medical record numbers, patient account numbers, case identification numbers, provider and doctor information and health record information, and Social Security numbers, which SSM then provided to Navvis in connection with Navvis' health

management operations.[19]

36. From July 12, 2023 to July 25, 2023, the Private Information of Plaintiffs and the Class Members, which they entrusted to SSM and which SSM provided to Navvis, was unauthorizedly disclosed to third-party cybercriminals during a cyberattack to Navvis' systems.

37. At some point in time, SSM posted a vague notification to its website, stating:

> **Data security breach information**
>
> Navvis & Company LLC (Navvis), a business partner that provides health management services to SSM Health, has recently experienced a data security incident that may have resulted in the compromise of protected health information for a limited number of SSM Health patients. Navvis has sent notice letters to these impacted individuals offering free credit monitoring and identity protection services. For more information please visit this Navvis site, or call 1-888-996-4022.[20]

38. The link SSM provided in its website notification redirected to Navvis' website, a Notice of Data Event posted by Navvis, on information and belief, on or about October 3, 2023 ("Website Notice").[21]

39. The Website Notice stated that:

> On July 25, 2023, Navvis & Company, LLC ("Navvis") became aware of suspicious activity on its computer network. Navvis immediately launched an investigation, to determine the nature and scope of the incident. Through its investigation, Navvis determined that, between July 12, 2023 – July 25, 2023, it was a victim of a cyber-attack, and a threat actor had access to certain systems that stored personal and protected health information.[22]

40. Navvis' website notice went onto explain that following its discovery of the Data

---

[19] *See* SSM Health, *Data security breach information,* available at https://www.ssmhealth.com/data-security-incidents-your-protected-health-information (last acc. Feb. 2, 2024).
[20] *See Id.*
[21] Navvis *Notice of Data Event*, available at https://navvishealthcare.com/privacy-update (last acc. Feb. 2, 2024) **Exhibit A.**
[22] *Id.*

Breach, Navvis "conducted a thorough forensics review of the systems and files to confirm what information was stored therein, and to whom the information related," which was completed on or about July 25, 2023 and which "identified certain individuals' information was present within the accessed records." [23]

41. Further, in its website notice, Navvis stated that the information compromised in the Data Breach include: an individual's name, date of birth, Medicaid/Medicare ID number, health plan information, medical treatment information, medical record number, patient account number, case identification number, provider and doctor information and health record information, and in some circumstances, Social Security number.[24]

42. On or about September 22, 2023, Navvis reported the Data Breach to the United States Department for Health and Human Services, Department for Civil Rights, stating that the Data Breach was a "Hacking/IT Incident" to a "Network Server" affecting 917 people.[25]

43. According to Navvis, as stated in December 29, 2023 report of the Data Breach to the Washington Attorney General, Navvis began sending written notice of the Data Breach to impacted persons on or about September 22, 2023; sent a second round of notifications on December 7, 2023; and sent written notice to other impacted persons on or about December 29, 2023 (collectively, "Data Breach Notices"). Navvis' report to the Washington Attorney indicated that "[t]he information that could have been subject to unauthorized access includes name, Social Security number, date of birth, diagnosis/clinical information, and medical treatment/procedure

---

[23] *Id.*
[24] *Id.*
[25] *See United States Department for Health and Human Services, Department for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last acc. Feb. 2, 2024).
[25] *See Id.*

information."[26]

44. In its mailed Data Breach Notices, Navvis explained that it "is in possession of your information because we are a provider of health management services to health care organizations, including SSM Health," and, vaguely explained the occurrence of the Data Breach as stated in the Website Notice, but further stated that in the unauthorized actor's access to certain systems "between July 12, 2023, and July 25, 2023 […] certain files and information within these systems may have been accessed, or acquired, by the unauthorized actor."[27]

45. In its Data Breach Notices, Navvis stated that, "[a]s part of our ongoing commitment to the security of information, we are reviewing and enhancing our already robust policies and procedures related to data privacy, to reduce the likelihood of a similar future event."[28]

46. Further, Navvis' Data Breach Notices recommended that individuals should "remain vigilant against incidents of identity theft and fraud, and to review your account statements and credit reports for suspicious activity and errors" and informed affected persons of their abilities to request free credit reports; place initial or extended fraud alerts on their credit files; and place credit freezes on their credit reports.[29]

47. Further still, Navvis offered individuals whose Private Information was affected in the Data Breach 12 months of credit monitoring and identity protection services through IDX.[30]

48. While Navvis' Website Data Breach Notice and mailed Data Breach Notices vaguely informed affected persons, Plaintiffs and the proposed Class Members, of the occurrence

---

[26] *See Navvis Report to the Washington Attorney General and sample Data Breach Notice,* available at https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachA27442.pdf (last acc. Feb. 2, 2024).
[27] *See* Data Breach Notices, Exhibits B and C.
[28] *Id*.
[29] *Id*.
[30] *Id*.

of the Data Breach as described above, neither informed them of exactly how the Data Breach occurred (i.e., an external system hack, ransomware attack, or phishing scheme); failed to state why it took Defendants so long to notify affected persons of the unauthorized disclosure; and minimized the severity of the Data Breach, stating that "[w]e are unaware of any actual misuse of your information at this time." [31]

49. On information and belief, Navvis did not have adequate security protocols to prevent, detect, and stop the cybercriminals from executing the cyberattack on its systems and accessing the voluminous Private Information of Plaintiffs and the proposed Class Members, provided to Navvis by SSM, which was stored on Navvis systems, in the Data Breach. Further, SSM failed to ensure that Navvis employed these adequate security protocols.

50. Further, Navvis failed to adequately train its employees on reasonable cybersecurity protocols and failed to implement reasonable security measures, causing it to lose control over its Plaintiffs' and the Class Members' Private Information in the Data Breach, and SSM failed to ensure that Navvis engaged in this adequate training and reasonable security measures.

51. Defendants' tortious conduct and breach of contractual obligations, as explained hereinafter, are evidenced by their failure to recognize the July 2023 Data Breach until cybercriminals had already accessed the data from Navvis' systems, meaning that Defendants had no effective means to detect and prevent attempted data breaches, or for SSM to ensure that Navvis employed such measures.

52. As a result of Defendants' Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their dates of birth and Social Security numbers. Accordingly, Navvis' credit monitoring and identity theft protection through

[31] *Id.*

IDX is wholly insufficient to compensate Plaintiffs and the Class Members for their damages which has been and imminently will be caused by the Data Breach.

53. Indeed, as a result of the Data Breach which Defendants permitted to occur by virtue of their inadequate data security practices, Plaintiffs and the proposed Class Members have suffered injury and damages, as set forth herein.

C. Plaintiffs' Experiences

Plaintiff John Doe

54. Plaintiff John Doe is a patient of SSM, having received medical care and treatment in 2023 at SSM Health Physical Therapy, SSM Health Saint Louis University Hospital, and other SSM medical facilities.

55. As a condition of receiving treatment, Plaintiff John Doe provided his Private Information to SSM, which SSM then provided to Navvis in connection with its health management services.

56. Plaintiff John Doe would not have provided his Private Information to SSM nor permitted SSM to provide this Private Information to Navvis in the absence of Defendants' representations and promises and mutual understanding that Defendants would safeguard his Private Information, in accordance with industry standard practices, Defendants' internal privacy policies, and the law.

57. Indeed, Plaintiff John Doe is very careful to guard the confidentiality of his Private Information, and never stores this information in an unsecure setting nor disseminates it publicly.

58. Plaintiff John Doe received Navvis' Data Breach Notice dated December 29, 2023.[32]

[32] *See* Data Breach Notice, **Exhibit B**.

59. According to the Data Breach Notice, Plaintiff John Doe's name, and Benefit Number, Date Of Birth, Diagnosis/Clinical Information, Health Insurance Policy-related Number, Medical Date of Service, Medical Provider Name, Medical Provider NPI, and Patient Account Number were unauthorizedly disclosed and accessed by cybercriminals in the Data Breach.

60. Upon information and belief, based on the nature of the cyberattack, Plaintiff John Doe's Private Information which was unauthorized disclosed to and obtained by cybercriminals in the Data Breach is being used, and/or will imminently be used, for fraudulent and criminal purposes, and has been or imminently will be published to and sold on the Dark Web for fraudulent purposes and sale.

61. As a direct result of the Data Breach that Defendants permitted to occur, Plaintiff John Doe has suffered injury-in-fact and damages, including: the unauthorized disclosure of Private Information itself, including on information and belief, publication to the Dark Web; dramatic increase in spam telephone calls, texts, and emails; and, he has been forced to expend time and effort to protect himself from identity theft resulting from the Data Breach, including, monitoring his credit reports and account statements, and will be required to do so into the future to mitigate the consequences of the Data Breach.

62. Further, Plaintiff John Doe fears for his personal financial security and uncertainty over the information disclosed in the Data Breach, and is experiencing emotional distress over the unauthorized disclosure of his Private Information. He is experiencing feelings of anxiety, embarrassment, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

63. Plaintiff John Doe was highly disturbed by the Data Breach's nature and the thought

of cybercriminals accessing his highly sensitive Private Information and the harm caused by the Data Breach. He was also outraged that Defendants took five (5) months to notify him of the Data Breach even as it was discovered on July 25, 2024.

64. As a result of Defendants' Data Breach, Plaintiff John Doe faces a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like his date of birth.

Plaintiff Jane Doe

65. Plaintiff Jane Doe is a patient of SSM, having received medical care and treatment at SSM medical facilities in St. Louis, Missouri.

66. As a condition of receiving treatment, Plaintiff Jane Doe provided her Private Information to SSM, which SSM then provided to Navvis in connection with its health management services.

67. Plaintiff Jane Doe would not have provided her Private Information to SSM nor permitted SSM to provide this Private Information to Navvis in the absence of Defendants' representations and promises and mutual understanding that Defendants would safeguard her Private Information, in accordance with industry standard practices, Defendants' internal privacy policies, and the law.

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

69. Plaintiff Jane Doe received Navvis' Data Breach Notice dated December 29, 2023.[33]

70. According to the Data Breach Notice, Plaintiff Jane Doe's name, and Benefit Number, Date of Birth, Diagnosis/Clinical Information, Health Insurance Policy-related Number,

[33] Data Breach Notice, Exhibit C.

Medical Dates of Service, Medical Provider Names, Medical Provider NPI, Medical Treatment/Procedure Information, Other Patient Identifier, Patient Account Number, and Subscriber Identification Number were unauthorizedly disclosed and accessed by cybercriminals in the Data Breach.

71. Upon information and belief, based on the nature of the cyberattack, Plaintiff Jane Doe's Private Information which was unauthorized disclosed to and obtained by cybercriminals in the Data Breach is being used, and/or will imminently be used, for fraudulent and criminal purposes, and has been or imminently will be published to and sold on the Dark Web for fraudulent purposes and sale.

72. As a direct result of the Data Breach that Defendants permitted to occur, Plaintiff Jane Doe has suffered injury-in-fact and damages, including: the unauthorized disclosure of Private Information itself, including on information and belief, publication to the Dark Web; dramatic increase in spam telephone calls, texts, and emails; and, she has been forced to expend time and effort to protect herself from identity theft resulting from the Data Breach, including, monitoring her credit reports and account statements, and will be required to do so into the future to mitigate the consequences of the Data Breach.

73. Further, Plaintiff Jane Doe fears for her personal financial security and uncertainty over the information disclosed in the Data Breach, and is experiencing emotional distress over the unauthorized disclosure of her Private Information. She is experiencing feelings of anxiety, embarrassment, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

74. Plaintiff Jane Doe was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive Private Information and the harm caused by the Data Breach. She was also outraged that Defendants took five (5) months to notify her of the Data Breach even as it was discovered on July 25, 2024.

75. As a result of Defendants' Data Breach, Plaintiff Jane Doe faces a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like her date of birth.

D. This Data Breach was Foreseeable by Defendants.

76. Plaintiffs and the proposed Class Members provided their Private Information to SSM, which SSM then provided to Navvis, with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

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

78. Defendants tortiously failed to take the necessary precautions required to safeguard and protect the Private Information of Plaintiffs and the Class Members from unauthorized disclosure, including SSM failing to ensure that Navvis implemented adequate security measures Defendants' actions represent a flagrant disregard of Plaintiffs' and the other Class Members' rights.

79. Plaintiffs and Class Members were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants 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.

80. 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."[34]

81. 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 creates significant cybersecurity vulnerabilities and makes it much easier for bad actors to find an entry point into the network." [35]

82. Cyber-attacks against healthcare organizations, such Defendants, 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…"[36]

83. In 2019, a record 1,473 data breaches occurred, resulting in approximately

[34] 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).
[35] *Id*.
[36] 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)

164,683,455 sensitive records being exposed, a 17% increase from 2018.[37]

84. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[38]

85. 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)."[39]

86. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including SSM and Navvis. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[40]

87. Furthermore, Defendants were 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.[41]

88. According to the U.S. Department for Health and Human Services' "2022

---

[37] 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)
[38] *Ibid.*
[39] *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).
[40] 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).
[41] 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.

Healthcare Cybersecurity Year in Review, and a 2023 Look-Ahead," "[h]ealthcare data breaches have doubled in 3 years."[42]

89. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including SSM and Navvis.

90. 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,

91. Private Information can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and medical records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

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

E. Defendants Failed to Comply with FTC Guidelines

93. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

[42] 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

According to the FTC, the need for data security should be factored into all business decision-making.

94. 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.[43]

95. 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.[44]

96. 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

[43] *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).
[44] *See id*.

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

98. Defendants failed to properly implement basic data security practices widely known throughout the industry, including SSM failing to ensure that Navvis implemented these practices. Defendants' 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.

99. Defendants were at all times fully aware of their obligations to protect the Private Information of SSM's patients that was entrusted to SSM and Navvis. Defendants were also aware of the significant repercussions that would result from their failure to do so.

F. Defendants Fails to Comply with Industry Standards

100. 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.

101. 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.[45]

102. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[46]

103. Upon information and belief, Navvis failed to meet the minimum standards of both

[45] *See* https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Apr. 14, 2023).
[46] Understanding The NIST Cybersecurity Framework, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Apr. 14, 2023).

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 Plaintiffs' and the proposed Class Members' Private Information, and SSM failed to ensure that Navvis implemented those standards, resulting in the Data Breach.

G. Defendants' Conduct Violates HIPAA and Evidences Its Insufficient Data Security

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

105. 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.

106. 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 Defendants 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).

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

108. Defendants breached their obligations to Plaintiffs and the Class Members and/or

were otherwise negligent and reckless because Navvis failed to properly maintain and safeguard its computer systems, network, and data, and SSM failed to ensure that Navvis did so. Defendants' 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);

l. SSM failing to ensure that Navvis implemented the above.

109. As the result of Defendants' violations, Defendants negligently and unlawfully failed to safeguard Plaintiffs' and the Class Members' Private Information.

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

110. 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.

111. 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.

112. This leads 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.

113. 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.[47]

114. Researchers have further found that at medical facilities that experience a data security incident, the incident leads to a deterioration in patient outcomes, generally.[48]

115. 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 access to a complete medical history and records; and

e. the indefinite loss of personal medical history.[49]

116. 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:

> 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.

---

[47] *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).

[48] *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).

[49] *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).

117. Data breaches represent a significant problem for patients who have already experienced the inconvenience and disruption associated with a cyber-attack.

I. The Data Breach Caused Plaintiffs and the Class Members Injury and Damages

118. Plaintiffs 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 Defendants, that has occurred, is ongoing, and/or imminently will occur.

119. As stated prior, in the Data Breach, unauthorized cybercriminals were able to access the Plaintiffs' 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.

120. The ramifications of Defendants' failure to keep Plaintiffs' 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 license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

121. Because Defendants failed to prevent the Data Breach, Plaintiffs 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. Plaintiffs and the Class Members have suffered, and will imminently suffer:

a. Increase in spam telephone calls, texts and emails;

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

c. The diminution in value of their Private Information;

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

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

f. 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;

g. Delay in receipt of tax refund monies;

h. Unauthorized use of stolen Private Information;

i. Emotional distress; and,

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

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

123. 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.[50]

124. 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.[51]

125. 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.

126. 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.

127. 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.

128. 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

[50] *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).
[51] *See* https://www.identitytheft.gov/Steps (last visited September 1, 2021).

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." [52]

129. 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.[53]

130. 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.

131. 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."[54]

132. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and

---

[52] *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).

[53] *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 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).

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

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.

133. 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.

134. 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.

135. Where the most Private Information belonging to Plaintiffs and Class Members was accessible from Defendants' 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 Plaintiffs and the Class Members are at an increased risk of fraud and identity theft for many years into the future.

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

137. 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."[55]

138. Social Security numbers are among the worst kind of Private Information to have

[55] 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).

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.[56]

139. 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.[57] 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.

140. 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."[58]

141. 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

---

[56] *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)

[57] *See id.*

[58] *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).

information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[59] Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is $50 per person and up.[60]

142. Accordingly, the Data Breach has caused Plaintiffs 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.

143. Defendants knew or should have known of these harms which would be caused by the Data Breach they permitted to occur, and strengthened their data systems accordingly.

CLASS ACTION ALLEGATIONS

144. Pursuant to Missouri Court Rule of Civil Procedure 52.08, Plaintiffs bring this class action individually and on behalf of the following proposed Class (the "Class"):

> All Missouri citizens whose Private Information was disclosed, compromised and/or potentially compromised in the Data Breach to Navvis' computer network between July 12, 2023 and July 25, 2023 including those who received notice of the Data Breach.

145. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which the Defendants or its parent has a controlling interest, and their current or former officers and directors; (3) persons who

---

[59] *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).

[60] *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).

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) Plaintiffs' counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

146. Plaintiffs and the Class Members satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Rule 52.08(a).

147. **Numerosity:** The exact number of Class Members is unknown but is estimated to be into the thousands of persons at this time, and individual joinder in this case is impracticable. Class Members can be easily identified through Defendants' records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

148. **Typicality:** Plaintiffs' claims are typical of the claims of other Class Members in that Plaintiffs, and the Class Members sustained damages arising out of Defendants' Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiffs and the Class Members sustained similar injuries and damages, as a result of Defendants' uniform illegal conduct.

149. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiffs have no interests that conflict with, or are antagonistic to those of, the Class, and Defendants have no defenses unique to Plaintiffs.

150. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

a. whether Defendants violated the laws asserted herein, and other statutory privacy and consumer protection laws;

b. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Private Information;

c. Whether SSM failed to properly supervise Navvis;

d. whether Defendants breached the duty to use reasonable care to safeguard Plaintiffs' and the Class's Private Information;

e. Whether Defendants breached their contractual promises to safeguard Plaintiffs' and the Class's Private Information;

f. whether Defendants were negligent *per se* in not complying with privacy laws;

g. whether Defendants knew or should have known their practices and representations related to the Data Breach, and Private Information were deceptive and unfair;

h. whether Defendants knew or should have known about the inadequacies of their data security policies and system and the dangers associated with storing sensitive Private Information;

i. whether Defendants failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and the other Class

Members' Private Information from unauthorized release and disclosure;

j. whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendants' computer and software systems to safeguard and protect Plaintiffs' and the other Class Members' Private Information from unauthorized release and disclosure;

k. whether Defendants took reasonable measures to determine the extent of the Data Breach after it was discovered;

l. whether Defendants' delay in informing Plaintiffs and the Class of the Data Breach was unreasonable;

m. whether Defendants' method of informing Plaintiffs and the Class of the Data Breach was unreasonable;

n. whether Defendants' conduct was deceptive, unfair, or unconscionable, or constituted unfair competition;

o. whether Defendants' conduct was likely to deceive the public;

p. whether Defendants are liable for negligence or gross negligence;

q. whether Defendants' conduct, practices, statements, and representations about the Data Breach of the Private Information violated applicable state laws;

r. whether Defendants knew or should have known their representations were false, deceptive, unfair, and misleading;

s. whether Plaintiffs and the Class were injured as a direct and proximate result of the Data Breach;

t. whether Plaintiffs and the Class were damaged as a proximate cause or

result of Defendants' breach of their contract with Plaintiffs and the Class;

u. whether Defendants' practices and representations related to the Data Breach that compromised the Private Information breached implied warranties;

v. what the proper measure of damages is; and

w. whether Plaintiffs and the Class Members are entitled to restitutionary, injunctive, declaratory, or other relief.

151. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Petition. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered, and uniformity of decisions ensured.

152. A class action is therefore superior to individual litigation because:

a. the amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendants' conduct economically feasible in

the absence of the class action procedural device;

b. individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

153. In addition to satisfying the prerequisites of Rule 52.08(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 52.08(b) because:

a. the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendants;

b. the prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

c. Defendants have acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief herein appropriate with respect to the proposed Class as a whole.

d. questions of law or fact common to the members of the class predominate over any questions affecting only individual members, and that a class action is superior to other available methods for the fair and efficient

adjudication of the controversy.

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

154. Plaintiffs and the members of Class incorporate the above allegations as if fully set forth herein.

155. Plaintiffs and members of the Class entrusted their Private Information to Defendants. Defendants owed to Plaintiffs and other members of the Class a duty to exercise reasonable care in handling and using the Private Information in their 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, and for SSM to ensure that Navvis implemented these industry-standard security measures.

156. Defendants owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their Private Information in accordance with state- of-the-art industry standards for data security would result in the compromise of that Private Information—just like the Data Breach that ultimately came to pass.

157. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Class's Private Information by disclosing and allowing access to patients' Private Information to unknown third parties and by failing to properly supervise both the way the Private Information was stored, used, and exchanged, those in its employ who made that happen, and failing to supervise business associates in possession of the Private Information.

158. Defendants owed to Plaintiffs and members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their PII under Mo. Stat. § 407.1500

et seq., other equivalent laws, and other laws as referred to herein. Defendants also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. These duties are required and necessary for Plaintiffs and members of the Class 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.

159. Defendants owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Plaintiffs and members of the Class were required to provide their personal information to SSM in order to receive medical treatment, and SSM provided this Private Information to Navvis in connection with its health management services to SSM.

160. The risk that unauthorized persons would try to gain access to the Private Information and misuse it was foreseeable. Given that Defendants holds vast amounts of Private Information, it was inevitable that unauthorized individuals would try to access Navvis' databases containing SSM's patients' Private Information—whether by malware or otherwise.

161. Private Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs and members of the Class and the importance of exercising reasonable care in handling it, and the importance of SSM supervising Navvis to ensure that Navvis exercised reasonable care in handling the Private Information.

162. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the

personal information and Private Information of Plaintiffs and the Class which actually and proximately caused the Data Breach and Plaintiffs' and the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and the other Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and the Class's injuries-in-fact.

163. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

164. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiffs' and members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation: increase in spam telephone calls, texts and emails; loss of the opportunity to control how Private Information is used; diminution in value of their Private Information; 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; Unauthorized use of stolen Private Information; emotional distress; increased risk of fraud and identity theft and, the continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Private Information in their possession.

165. As a result, Plaintiffs and the Class Members are entitled to actual and compensatory damages, as well as punitive damages, as permitted by law.

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

166. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

146. Plaintiffs incorporates all previous paragraphs as if fully set forth herein.

147. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information, including the duty of SSM to ensure Navvis provided fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information,

148. 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 Defendants, 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 Defendants' duty to protect Plaintiffs' and the Class Members' sensitive Private Information.

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

150. Defendants violated their duties under Section 5 of the FTC Act, as well as HIPAA, by failing to use reasonable measures to protect Plaintiffs' and the Class's Private Information and not complying with applicable industry standards as described in detail herein. Defendants'

conduct was particularly unreasonable given the nature and amount of Private Information SSM had collected, given to Navvis, 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.

151. 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 Plaintiffs and members of the Class.

152. Defendants had a duty to Plaintiffs and the Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and the Class's Private Information and of SSM to supervise Navvis to ensure it implemented and maintained reasonable security procedures and practices to safeguard Plaintiffs' and the Class's Private Information.

153. Defendants breached their respective duties to Plaintiffs 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 Plaintiffs' and Class Members' Private Information, and to supervise their vendors to ensure they did so.

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

155. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiffs and members of the Class, Plaintiffs and Class Members would not have been injured.

156. The injury and harm suffered by Plaintiffs and Class Members was the reasonably

foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiffs and Class Members to suffer the foreseeable harms associated with the exposure of their Private Information.

157. Had Plaintiffs and Class Members known that Defendants did not adequately protect their Private Information, and that SSM did not ensure that Navvis adequately protected this information, Plaintiffs and Class Members would not have entrusted Defendant with their Private Information, or permitted SSM to entrust that information to Navvis.

158. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will imminently suffer, actual, tangible, injury-in-fact and damages, including, without limitation: increase in spam telephone calls, texts and emails; loss of the opportunity to control how Private Information is used; diminution in value of their Private Information; 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; Unauthorized use of stolen Private Information; emotional distress; increased risk of fraud and identity theft and, the continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Private Information in their possession.

159. Plaintiffs and the Class Members are entitled to compensatory, actual, and punitive damages as a result of the Data Breach.

COUNT III
INVASION OF PRIVACY

(On Behalf of the Plaintiffs and the Class)

167. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

168. Defendants publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiffs and the Class by disclosing and exposing Plaintiffs' and Class's Private Information to enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the dark web and elsewhere.

169. The disclosure of the Private Information, including patients' names, dates of birth, Medicaid/Medicare ID numbers, health plan information, medical treatment information, medical record numbers, patient account numbers, case identification numbers, provider and doctor information and health record information, and Social Security numbers, is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

170. Defendants have extensive knowledge of their patients' medical conditions and SSM undertook to provide medical care for them, with the assistance of Navvis, and therefore Defendants have a special relationship with Plaintiffs and the Class and Defendants' disclosure of Private Information is certain to embarrass them and offend their dignity. Defendants should appreciate that the cyber- criminals who stole the Private Information would further sell and disclose the Private Information as they are doing. That the original disclosure is devastating to the Plaintiffs and the Class, even though it originally may have only been disclosed to one person or a limited number of cyber-criminals, does not render it any less a disclosure to the public-at-large.

171. Missouri Courts, and courts of other states, have recognized a cause of action for an invasion of privacy for over a century. *See, e.g., Sullivan v. Pulitzer Broad. Co.*, 709 S.W.2d

475, 477 (Mo. 1986) (citing *Munden v. Harris*, 153 Mo. App. 652, 134 S.W. 1076 (1911)). Plaintiffs' and the Class's PII was publicly disclosed by Defendants in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendants knew and know that Plaintiffs' and Class's Private Information is not a matter of legitimate public concern.

172. As a direct and proximate result of Defendants' conduct, Plaintiffs and members of the Class have suffered tangible injury-in-fact and damages, including without limitation: increase in spam telephone calls, texts and emails; loss of the opportunity to control how Private Information is used; diminution in value of their Private Information; 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; Unauthorized use of stolen Private Information; emotional distress; increased risk of fraud and identity theft and, the continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Private Information in their possession.

173. Plaintiffs and the Class Members are entitled to compensatory, actual, and punitive damages as a result of Defendants' invasion of privacy in the Data Breach.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of the Plaintiffs and the Class)

174. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

175. Defendants offered to provide medical services to Plaintiffs and members of the Class in exchange for payment and their Private Information.

176. Plaintiffs and the Class accepted Defendants' offer and paid money to SSM and/or Navvis and provided Defendants with their Private Information.

177. Plaintiffs and members of the Class exchanged valuable consideration – money – with Defendants for medical services, a portion of which was for reasonable data security.

178. A crucial part of the contract was Defendants' implicit promise to protect Plaintiffs' and the Class's Private Information from unauthorized disclosure.

179. In its Notice of Privacy Practices, Defendants expressly promised Plaintiffs and the Class that Defendants would only disclose (share) PHI/ Private Information under certain circumstances, none of which relate to the Data Breach.

180. Necessarily implicit in the agreement(s) between Defendants and its patients, including Plaintiffs and members of the Class, were Defendants' obligation to use such Private PHI/Information for permissible purposes only, such as for treatment or health care operations, to take reasonable steps to secure and safeguard that Private Information, and not make disclosures of the Private Information to unauthorized third parties.

181. Further implicit in the agreement, and stated in SSM's Notice of Privacy Practices, Defendants were obligated to provide Plaintiffs and members of the Class with prompt and adequate notice of any and all unauthorized access and/or theft of their Private Information.

182. Plaintiffs and members of the Class would not have entrusted their sensitive Private Information to Defendants in the absence of such agreement with Defendants.

183. Defendants materially breached the implied contract(s) they had entered with Plaintiffs and members of the Class by failing to safeguard such Private Information and failing to

notify them promptly of the intrusion into Navvis' computer systems that compromised such information.

184. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendants' material breaches of their agreements.

185. Plaintiffs and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendants.

186. Under the laws of Missouri and other states, good faith 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.

187. 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.

188. Defendants failed to promptly advise Plaintiffs and members of the Class of the Data Breach.

189. In these and other ways, Defendants violated their duty of good faith and fair dealing.

190. Plaintiffs and members of the Class have sustained damages as a result of Defendants' breaches of its agreement, including breaches thereof through violations of the

covenant of good faith and fair dealing.

COUNT V
UNJUST ENRICHMENT
(On Behalf of the Plaintiffs and the Class)

191. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

192. This claim is pled in the alternative to the breach of implied contractual duty claim.

193. Plaintiffs and members of the Class conferred a monetary benefit upon Defendants in the form of monies paid for medical treatment.

194. Defendants appreciated or had knowledge of the benefits conferred upon themselves by Plaintiffs and members of the Class. Defendants also benefited from the receipt of Plaintiffs' and the Class's Private Information, as this was used to facilitate the provision of medical treatment.

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

196. Under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and members of the Class because Defendants failed to implement, adequately implement, and/or SSM failed to ensure that Navvis implement, the data privacy and security practices and procedures for itself that Plaintiffs and the Class paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

197. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it as a result

of the conduct and Data Breach alleged herein.

COUNT VI
VIOLATION OF THE MISSOURI MERCHANDISING PRACTICES ACT (MMPA)
Mo. Stat. § 407.010, *et seq.*
(On Behalf of the Plaintiffs and the Class)

198. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

199. Defendants were each engaged in the sale of a "merchandise" in "trade" or commerce" as defined under the MMPA.

200. Defendants' business of providing medical services was primarily for "personal," "family," or "household" purposes.

201. Plaintiffs and members of the Class purchased Defendants' medical services when Plaintiffs and the members of the Class paid Defendants for these services.

202. As part of that transaction, Defendants required Plaintiffs and the Class to provide Defendants with their Private Information, including names, dates of birth, Medicaid/Medicare ID numbers, health plan information, medical treatment information, medical record numbers, patient account numbers, case identification numbers, provider and doctor information and health record information, and Social Security numbers.

203. As recounted above, the value of Plaintiffs' and Class's Private Information is considerable. Hence, Plaintiffs and members of the Class would not have handed over that Private Information absent representation and assurances from Defendants that the Private Information would be secure.

204. Defendants failed to reveal material facts in connection with the sale and advertisement of their services in violation of the MMPA, including but not limited to the following:

- Failing to maintain sufficient data security to keep Plaintiffs' and Class's sensitive Private Information secure, including SSM failing to ensure that Navvis maintained sufficient data security;
- Misrepresenting material facts to the class, in connection with the sale of goods and services by representing that SSM would "[m]ake sure that medical information that identifies you is kept private" and to safeguard Plaintiffs' and Class's Private Information from unauthorized disclosure, release, data breaches and theft.
- Misrepresenting material facts to Plaintiffs and members of the Class in connection with sale of goods and services by representing that SSM did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and the Class's Private Information.
- Failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and Class's Private Information from further unauthorized disclosure, release, data breaches, and theft.

205. In addition, Defendants' failure to disclose that their and/or Navvis' computer systems were not well- protected, and that Plaintiffs' and the Class's Private Information was vulnerable and susceptible to intrusion while it was entrusted to Defendants, constitutes deceptive and/or unfair acts or practices because Defendants knew such facts would (a) be unknown to and not easily discoverable by Plaintiffs and the Class; and (b) defeat Plaintiffs' and the Class's ordinary, foreseeable, and reasonable expectations concerning the security of their PII.

206. Defendants also engaged in unfair acts and practices by failing to maintain the privacy and security of Plaintiffs' and the Class's Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

207. Defendants' wrongful practices occurred in the course of trade or commerce.

208. As a direct and proximate result of Defendants' violations of the Missouri Merchandising Practices Act, Plaintiffs and the Class have suffered injury-in-fact and damages, including but not limited to increase in spam telephone calls, texts and emails; loss of the opportunity to control how Private Information is used; diminution in value of their Private Information; 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; Unauthorized use of stolen Private Information; emotional distress; increased risk of fraud and identity theft and, the continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Private Information in their possession.

209. Plaintiffs and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the MMPA.

PRAYER FOR RELIEF

Plaintiffs, JOHN DOE and JANE DOE, individually, and on behalf of all others similarly situated, demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding Plaintiffs and the Class damages that include compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest, in an amount to be proven at trial;

C. Awarding restitution and damages to Plaintiffs 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 Plaintiffs and the Class;

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

F. Enjoining Defendants from further deceptive and unfair practices and making untrue statements about the Data Breach and the stolen Private Information;

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

H. Granting Plaintiffs and the Class leave to amend this petition 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

Plaintiffs demand a trial by jury on all issues so triable.

Dated: February 2, 2024

Respectfully submitted,

/s/ John F. Garvey

John F. Garvey #35879
Colleen Garvey #72809
Ellen A. Thomas #73043
STRANCH, JENNINGS & GARVEY, PLLC
701 Market Street
Peabody Plaza, Suite 1510
St. Louis, MO 63101
(314) 390-6750
jgarvey@stranchlaw.com
cgarvey@stranchlaw.com
ethomas@stranchlaw.com

Counsel for Plaintiffs and the Proposed Class

Certificate of Filing

The undersigned hereby certifies that the foregoing Class Action Petition has been filed by using the Court's electronic case filing system on this 2nd day of February, 2024.

/s/John F. Garvey

ClassAction.org