IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

In re:	Case No. 4:24-cv-00029-AGF
Navvis & Company, LLC Data Breach Litigation	**JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Dorothy Winston, Melanie Burns, Donna Allen, Duane Zellmer, Julie Montiel, on behalf of her minor child, E.C., Julie Schaus, Keeley Bogart, Richard Lilly, and Jeff Ruderman ("Plaintiffs"), individually and on behalf of all others similarly situated (the "Class" or "Class Members"), bring this Consolidated Class Action Complaint (the "Complaint") against Defendant Navvis & Company, LLC, d/b/a Navvis ("Defendant" or "Navvis"). The allegations set forth in this Complaint are based on the personal knowledge of the Plaintiffs, upon information and belief, and further investigation of counsel.

I. NATURE OF THE ACTION

1. This is a data breach class action against Defendant for its failure to adequately secure and safeguard confidential and sensitive information of Plaintiffs and the Class held throughout the typical course of Defendant's business.

2. Between July 12 and July 25, 2023, an unauthorized third-party actor gained access to the Defendant's network and computer systems and obtained unauthorized access to Defendant's files (the "Data Breach").

3. Upon information and belief, thousands of individuals and their information was stolen in the Data Breach. Defendant has not yet disclosed the exact number of individuals impacted by the Data Breach. The information exposed or otherwise accessed by an unauthorized

third-party in the Data Breach included Plaintiffs' and Class Members' Personally Identifiable Information ("PII") and Protected Health Information ("PHI"), including names, dates of birth, Beneficiary HIC numbers, medical dates of service, patient account numbers, diagnosis/clinical information, health insurance policy-related number, medical provider name, medical provider NPI, medical treatment/procedure information, other patient identifiers, and Subscriber ID's (collectively, "Private Information").

4. Defendant learned of the Data Breach on or about July 25, 2023.

5. After learning of the breach, Defendant conducted an investigation and engaged outside cybersecurity professionals and data privacy counsel. Defendant, so far, has yet to inform affected individuals when it completed its investigation or when it completely learned of the extent of the Data Breach.

6. On or about December 29, 2023, and February 9, 2024, Defendant began notifying affected individuals that their Private Information was stolen in the Data Breach. Although Defendant learned of the Data Breach in July of 2023, it waited over five (5) months to begin notifying affected individuals of the Data Breach.

7. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiffs and the Class, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

8. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality and security of their Private Information.

9. Plaintiffs and the Class reasonably expected Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes

only, and to make only authorized disclosures of this information.

10. Defendant, however, breached its numerous duties and obligations by failing to implement and maintain reasonable safeguards; failing to comply with industry-standard data security practices and federal and state laws and regulations governing data security; failing to properly train its employees on data security measures and protocols; failing to timely recognize and detect unauthorized third parties accessing its system and that substantial amounts of data had been compromised; and failing to timely notify the impacted Class.

11. In this day and age of regular and consistent data security attacks and data breaches, in particular in the healthcare industry, and given the sensitivity of the data entrusted to Defendant, this Data Breach is particularly egregious and foreseeable.

12. By implementing and maintaining reasonable safeguards and complying with standard data security practices, Defendant could have prevented this Data Breach.

13. Plaintiffs and the Class are now faced with a present and imminent lifetime risk of identity theft or fraud. These risks are made all the more substantial, and significant, because many Class Members' Private Information has already been actually misused and found on the dark web.

14. Private Information has great value to cyber criminals. As a direct cause of Defendant's Data Breach, Plaintiffs' and the Class Members' Private Information was stolen and is now in the hands of cyber-criminals and, in some instances, is already available for sale on the dark web for other criminals to access and abuse at the expense of Plaintiffs and the Class. Plaintiffs and the Class now face a current and lifetime risk of identity theft or fraud as a direct result of the Data Breach.

15. Upon information and belief, Defendant acknowledges the imminent threat the Data Breach has caused to Plaintiffs.

16. The modern cyber-criminal can use the Private Information and other information stolen in the Data Breach to assume a victim's identity when carrying out various crimes such as:

a. Obtaining and using a victim's credit history;

b. Publishing and selling a victim's Private Information on the dark web;

c. Making financial transactions on their behalf and without their knowledge or consent, including opening credit accounts in their name or taking out loans;

d. Impersonating them in written communications, including mail, e-mail, and/or text messaging;

e. Stealing, applying for and/or using benefits intended for the victim;

f. Committing illegal acts while impersonating their victim which, in turn, could incriminate the victim and lead to other legal ramifications.

17. Plaintiffs' and Class Members' Private Information was stolen due to Defendant's negligent and/or careless acts and omissions and the failure to protect Plaintiffs' and Class Members' Private Information. Defendant not only failed to prevent the Data Breach, but after discovering the Data Breach in July of 2023, waited until on or around December 29, 2023, to begin notifying affected individuals such as Plaintiffs and members of the Class. Even more disconcerting is the fact that Defendant sent out additional notice letters to certain Plaintiffs and Class Members on or around February 9, 2024. Therefore, for nearly seven (7) months many Class Members remained unaware that their Private Information was stolen in the Data Breach.

18. As a result of Defendant's delayed response to the Data Breach, Plaintiffs and the Class had no idea their Private Information had been stolen, and that they were, and continue to be, at significant and imminent risk of identity theft, fraud, and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes because of

Defendant's negligence.

19. Plaintiffs bring this action on behalf of all persons whose Private Information was stolen in the Data Breach as a direct consequence of Defendant's failure to:

(i) adequately protect consumers' Private Information entrusted to it,

(ii) warn its current and former customers, as well as potential customers of their inadequate information security practices, and

(iii) effectively monitor their websites and platforms for security vulnerabilities and incidents.

20. Defendant's conduct amounts to negligence and violates federal and state statutes and guidelines.

21. As a result of the Data Breach, Plaintiffs and the Class suffered ascertainable losses, including but not limited to, a loss of privacy. These injuries include:

(i) the invasion of privacy;

(ii) the compromise, disclosure, theft, and imminent unauthorized use of Plaintiffs' and Class Members' Private Information;

(iii) the publishing of Plaintiffs' and Class Members' Private Information to the dark web;

(iv) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their Private Information;

(v) lost or diminished inherent value of their Private Information;

(vi) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;

(vii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time or wages;

(viii) the continued and increased risk to their Private Information, which, (a) is available on the dark web for individuals to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and the Class.

22. Defendant has offered abbreviated, non-automatic, single bureau credit monitoring services to victims thereby identifying the harm posed to Plaintiffs and Class Members as a result of the Data Breach, which does not adequately address the lifelong harm that victims face following the Data Breach. Indeed, the Data Breach involves Private Information that cannot easily be changed.

23. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security practices employed by Defendant.

24. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert the claims alleged below. Plaintiffs also seek injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity by law, or any other relief the Court deems just and appropriate.

II. PARTIES

25. Plaintiff **Dorothy Winston** is, and at all relevant times was, a citizen of Forest Park,

Oklahoma.

26. Plaintiff **Melanie Burns** is, and at all relevant times was, a citizen of Oklahoma City, Oklahoma.

27. Plaintiff **Donna Allen** is, and at all relevant times was, a citizen of Osage Beach, Missouri.

28. Plaintiff **Duane Zellmer** is, and at all relevant times was, a citizen of Seffner, Florida.

29. Plaintiff **Julie Montiel**, on behalf of her minor child, E.C., is, and at all relevant times was, a citizen of Baraboo, Wisconsin.

30. Plaintiff **Julie Schaus** is, and at all relevant times was, a citizen of Dane County, Wisconsin.

31. Plaintiff **Keeley Bogart** is, and at all relevant times was, a citizen of Madison County, Illinois.

32. Plaintiff **Richard Lilly** is, and at all relevant times was, a citizen of Cole County, Missouri.

33. Plaintiff **Jeff Ruderman** is, and at all relevant times was, a citizen of Livingston, New Jersey.

34. Defendant **Navvis & Company LLC's** principal place of business is located at 555 Maryville University Drive, Suite 240, St. Louis, MO 63141.

III. JURISDICTION AND VENUE

35. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), *et seq*. The amount in controversy exceeds $5 million, exclusive of interest and costs. There are more than 100 members in the proposed Class, and at least one

member of the Class is a citizen of a state different from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

36. This Court has personal jurisdiction over Defendant because Defendant's principal places of business is located within this District and the Defendant conducts substantial business in this district.

37. Venue is proper in this Court under 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District, and Defendant resides within this judicial district.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business

38. Defendant is a healthcare company specializing in "working with health plans, health systems, and physician enterprises to build, operate, and manage new business models that accelerate and fundamentally change the way healthcare is delivered."[1]

39. In the ordinary course of its business practices, Defendant stores, maintains, and uses Plaintiffs' and Class Members' Private Information, which includes but is not limited to information such as:

a. Names;

b. Beneficiary HIC numbers;

c. Dates of birth;

d. Diagnosis/Clinical Information;

e. Health Insurance Policy-related numbers;

f. Medical dates of service;

[1] https://www.navvishealthcare.com/about-navvis/

g. Medical provider names;

h. Medical provider NPI;

i. Medical treatment/procedure information;

j. Other patient identifiers;

k. Patient account numbers; and

l. Subscriber ID.

40. Defendant understands the importance of securely storing and maintaining Private Information.

41. In fact, Defendant's privacy policy "recognizes that the privacy of…personal information is important…."[2] As such, Defendant promised to only share Private Information with "third parties who perform functions or services on [Navvis's] behalf as outlined in this Privacy Policy and otherwise as permitted by law."[3]

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

43. Plaintiffs and Class Members provided their Private Information, directly or indirectly, to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

---

[2] https://www.navvishealthcare.com/legal/#:~:text=We%20collect%20and%20may%20use,services%20and%20to%20improve%20the

[3] *Id*.

44. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

45. Defendant had obligations created by the FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

46. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without requiring the submission of Plaintiffs' and the Class Members' Private Information, Defendant could not perform the services it provides.

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

48. Defendant breached these duties owed to Plaintiffs and Class Members by enabling an unauthorized actor to access its systems and steal certain files containing Plaintiffs' and Class Members' Private Information, which has now been found on the dark web.

B. The Data Breach

49. Defendant became aware of the Data Breach on or about July 25, 2023, when it identified suspicious activity within its computer network environment.

50. In response, Defendant attempted to remedy the Data Breach by taking steps to

secure its systems and network, launching its own, independent review to investigate the matter further.

51. Through Defendant's own investigation, it discovered that beginning on July 12, 2023, through July 25, 2023, an unauthorized actor had accessed and acquired files within Defendant's systems. The stolen files contained Plaintiffs' and Class Members' Private Information.

52. Despite learning of the Data Breach on July 25, 2023, Defendant waited over five (5) months after learning of the Data Breach to begin notifying affected individuals, including Plaintiffs and Class Members.

53. Upon information and belief, Defendant did not begin the process of notifying Plaintiffs and Class Members until on or around December 29, 2023, with additional notice letters circulated months later on or around February 9, 2024.

54. Additionally, although Plaintiffs and Class Members have an interest in ensuring that their information remains protected, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures taken by Defendant to ensure a data breach does not occur again have not been shared with regulators, Plaintiffs, or Members of the Class.

55. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

56. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they collected from Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no

longer needed.

57. Now, as a result of the Data Breach, Plaintiffs' and Class Members' Private Information has been misused and found on the dark web.

C. Defendant Acquires, Collects, and Stores Consumers' Private Information

58. As a condition to obtain healthcare business services from Defendant, Plaintiffs and Class Members were required to give their sensitive and confidential Private Information, directly or indirectly, to Defendant.

59. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiffs' and Class Members' Private Information, Defendant would be unable to perform its services and earn its profits.

60. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

61. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

62. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

63. Upon information and belief, Defendant made promises to Plaintiffs and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

64. These promises included those found in Defendant's privacy policy, which "recognizes that the privacy of…personal information is important…."[4] Further, Defendant promised to only share Private Information with "third parties who perform functions or services on [Navvis's] behalf as outlined in this Privacy Policy and otherwise as permitted by law."[5]

65. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed at Defendant to protect and secure sensitive data.

D. Defendant Was Aware of the Data Breach Risks

66. In light of recent high-profile data breaches at other companies in the healthcare industry, Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

67. As a large national business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which Defendant was aware and knew it had a duty to guard against. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the period of 2019 - 2020.[6]

---

4 https://www.navvishealthcare.com/legal/#:~:text=We%20collect%20and%20may%20use,services%20and%20to%20improve%20the

5 *Id*.

6 *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Feb. 29, 2024).

68. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced cyberattacks, resulting in 66,658,764 individuals' personal information being compromised.[7]

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

70. Defendant had and continues to have obligations created by implied contract, industry standards, common law, and representations made to Plaintiffs and the Class, to keep their Private Information private and confidential and to protect it from unauthorized access, exfiltration, and theft.

71. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and data breaches in the healthcare industry preceding the date of the Data Breach. Further, due to the sensitive Private Information retained, healthcare companies are an "easy target" for cyberattacks.[8]

72. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and foreseeable to the public and to anyone in Defendant's industry, including Defendant.

73. Additionally, as companies become more dependent on computer systems to run their business,[9] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need

[7] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Oct. 11, 2023).
[8] *See* https://www.hipaajournal.com/why-do-criminals-target-medical-records/
[9] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

for adequate administrative, physical, and technical safeguards.[10]

74. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take substantial time, money, and patience to resolve.[11] Identity thieves use the stolen Private Information for a variety of crimes, including but not limited to, credit card fraud, telephone or utilities fraud, and bank and finance fraud.[12]

75. In the notice letter, Defendant makes an offer of 12 months of credit monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' Private Information. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity and credit monitoring services.

76. Defendant's offer of credit monitoring establishes that Plaintiffs' and Class Members' Private Information *was* accessed and stolen by cyber criminals for the very purpose of engaging in illegal and unethical conduct, including crimes involving identity theft, fraud, or to otherwise profit by selling their data to other criminals who purchase Private Information for that

---

[10] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

[11] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf (last visited Feb. 29, 2024).

[12] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

purpose. In addition to the actual misuse that has already occurred, fraudulent activity resulting from the Data Breach may not come to light for years.

77. Defendant knew, or should have known, the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of the Data Breach.

78. Plaintiffs and the Class now face years of constant monitoring and surveillance of their financial and personal records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information as a direct result of the Data Breach.

79. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's own failure to install, implement, and maintain adequate data security measures, software, and other industry best practices for safeguarding the Private Information of Plaintiffs and the Class.

80. As a healthcare company in possession of consumers' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

E. Defendant Failed to Comply with FTC Guidelines

81. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable and adequate data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

82. In 2022, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' 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.[13]

83. The FTC further recommends that companies not maintain Private Information 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.

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

[13] Ritchie, J. N. & A., & Jayanti, S.F.-T. and A. (2022, April 26). *Protecting personal information: A guide for business.* Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed October 27, 2023)

85. These FTC enforcement actions include actions against healthcare companies, like Defendant.

86. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

87. To prevent and detect cyber-attacks, including the cyber-attack on Defendant's system that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government and FTC, the following measures:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of malware and how it is delivered;

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound emails using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;

d. Configure firewalls to block access to known malicious IP addresses;

e. Patch operating systems, software, and firmware on devices using a centralized patch management system;

f. Set anti-virus and anti-malware programs to automatically conduct regular

scans and/or repairs;

g. Create and manage the use of privileged accounts based on the varying level of accessibility using a principle of least privilege: wherein no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary, such as any internal IT employees;

h. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares;

i. Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common malware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used;

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;

m. Execute operating system environments or specific programs in a virtualized environment; and

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

88. Defendant was at all times fully aware of its obligation to protect the Private Information of the individuals in its network. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Defendant Failed to Comply with Industry Standards

89. As shown above, experts studying cyber security routinely identify healthcare companies, like Defendant, as being particularly vulnerable to cyberattacks because of the value of their Private Information which they collect and maintain.

90. Several industry best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices. Best cybersecurity practices that are standard in the health management services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

91. Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards,

thereby opening the door to the cyber-attack and causing the Data Breach.

G. The Private Information Stolen in the Data Breach Holds Value to Cyber Criminals

92. Businesses, such as Defendant, that store Private Information in their daily course of business are more likely to be targeted by cyber criminals. Credit card, routing, bank account and other financial numbers are highly sought data targets for hackers, but the Private Information involved in the Data Breach is also, if not more, desirable to cyber criminals, as it can be easily used to perpetrate acts of identity theft and other types of fraud.

93. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web to obtain Private Information of other unknown individuals. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII and PHI can be sold at a price ranging from $40 to $200, and banking details have a price range of $50 to $200.[14]

94. In fact, healthcare records, which is a form of PHI stolen in the Data Breach, are worth $250.15 on average when sold, which "shows the dramatic difference in value of healthcare data when compared to other forms of private information that is commonly stolen and sold."[15] Further, clever hackers can use other medical data stolen in the Data Breach, including medical diagnosis information, to "obtain fraudulent prescriptions or even purchase medical equipment, which can later be sold for a profit."[16]

---

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web- how-much-it-costs (last visited Apr. 7, 2021).

[15] *See* https://www.accountablehq.com/post/why-is-phi-valuable-to-hackers (last accessed: March 4, 2024).

[16] *See* https://cloudtweaks.com/2016/07/hackers-interested-medical-data/#:~:text=Clever%20hackers%20can%20use%20an,later%20sold%20for%20a%20profit (last accessed: March 4, 2024).

95. The theft of Plaintiffs' and Class Members' Private Information left cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential information that can be used to mimic the identity of the victim. The Private Information of Plaintiffs and the Class stolen in the Data Breach constitutes a dream for hackers or cyber criminals and a nightmare for Plaintiffs and the Class.

96. The FTC has released its updated publication on protecting Private Information for businesses, which includes instructions on protecting Private Information, properly disposing of Private Information, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

97. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

98. Companies recognize that Private Information is a valuable asset and a valuable commodity, but also necessary throughout the typical course of business with consumers. Receiving Private Information is the receipt of value for a business such as Defendant.

99. Identity thieves may commit various types of crimes such as impersonate patients

[17] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29.

to get medical services, sell the Private Information on the dark web, demand a ransom, commit immigration fraud, obtain a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

100. Based on the foregoing, the Private Information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because those victims can file disputes, cancel or close credit and debit cards and/or accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not nearly impossible, to change.

H. Defendant's Conduct Violates HIPAA and is Evidence of Defendant's Insufficient Data Security.

101. Defendant is either a covered entity or a business associate under the Health Insurance Portability and Accountability Act ("HIPAA"), and as such is subject to the regulations under the statute.

102. HIPAA requires covered entities and business associates to protect against reasonably anticipated threats to the security of sensitive patient health information.

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

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

promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.304, 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).

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

> A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

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

I. Plaintiffs' and Class Members' Damages

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

108. Defendant has failed to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and the Class's Private Information other than offering twelve (12) months of complimentary credit-monitoring services to individuals involved in the Data Breach.

109. Plaintiffs and the Class have been damaged by the theft of their Private Information in the Data Breach, including actual misuse of their Private Information in the form of identity theft and financial fraud and being published to the dark web. Further, additional unencrypted Private Information stolen in the Data Breach will end up for sale on the dark web as that is the *modus operandi* of hackers.

110. Plaintiffs and the Class presently face a substantial risk of out-of-pocket fraud and losses such as unauthorized transactions, loans opened in their names, tax return fraud, utility bills

opened in their names, credit card fraud, and similar identity theft.

111. Plaintiffs and the Class have been, and currently face substantial risk of being targeted now and in the future, to phishing, data intrusion, and other illegality based on their Private Information being compromised in the Data Breach as potential fraudsters could use the information garnered to target such schemes more effectively against Plaintiffs and the Class.

112. Plaintiffs and the Class may also incur out-of-pocket costs for implementing protective measures such as purchasing credit and identity theft monitoring fees, credit report fees, credit freeze fees, and other similar costs directly or indirectly related to the Data Breach.

113. Plaintiffs and the Class also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

114. Plaintiffs and the Class have spent and will continue to spend significant amounts of uncompensated time monitoring their financial accounts, medical accounts, sensitive information, credit score, and other records for misuse.

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

116. In fact, Defendant's Notice Letter instructs Plaintiffs and Class Members to do the following:

> We encourage you to remain vigilant against incidents of identity theft and fraud, and to review your account statements and credit reports for suspicious activity and errors. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and file a request for help.

117. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter as well as monitoring their financial accounts for unauthorized activity, which may take years to discover and detect.

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

119. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety and fear that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, whether physically or virtually, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever. This is especially true considering Plaintiffs' and Class Members' Private Information has been used to commit identity theft and fraud and has already been located on the dark web.

120. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and the Class have suffered actual misuse of their Private Information, lost time and effort, anxiety, emotional distress, and loss of privacy, and are at an imminent, increased risk of future harm because of the Data Breach.

Plaintiff Dorothy Winston's Experience

121. Plaintiff Dorothy Winston is an adult individual and a natural person of Oklahoma, residing in Oklahoma County, where she intends to stay.

122. Plaintiff Winston provided her Private Information to Defendant with the reasonable expectation that Defendant would take reasonable precautions to protect her confidential Private Information.

123. Plaintiff Winston received a notice letter from Defendant dated December 29, 2023, informing her of the Data Breach and the exposure of her Private Information.

124. The notice letter informed Plaintiff Winston that her name, Bene HIC number, date of birth, diagnosis/clinical information, health insurance policy-related number, medical date of service, medical provider name, medical provider NPI, medical treatment/procedure information, other patient identifiers, patient account number, and subscriber ID had been stolen in the Data Breach.

125. Plaintiff Winston is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Winston diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her Plaintiff Winston uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

126. Plaintiff Winston only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff Winston's Private Information was within the possession and control of Defendant at the time of the Data Breach.

127. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Winston suffered injury from a loss of privacy.

128. Plaintiff Winston has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff Winston was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

129. Upon information and belief, Plaintiff Winston's Private Information has already been stolen and misused as she has been notified that her Private Information was found on the dark web. Specifically, after the Data Breach, on January 11, 2024, Plaintiff Winston received an alert from her IDX account that her Private Information was found on the dark web. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

130. Furthermore, Plaintiff Winston experiences daily spam calls, text messages, and emails as a result of the Data Breach.

131. The Data Breach has also caused Plaintiff Winston to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being found on the dark web and placed in the hands of criminals.

132. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Winston to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, contacting Defendant, setting up IDX credit monitoring, reviewing her IDX account, and regularly self-

monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

133. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Winston to suffer stress, fear, and anxiety.

134. Plaintiff Winston has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches

Plaintiff Melanie Burns's Experience

135. Plaintiff Melanie Burns is an adult individual and a natural person of Oklahoma, residing in Oklahoma County, where she intends to stay.

136. Plaintiff Burns received a notice letter from Defendant informing her of the Data Breach and the exposure of her Private Information.

137. The notice letter informed Plaintiff Burns that her name, Bene HIC Number, date of birth, medical date of service, and Patient Account number was stolen in the Data Breach.

138. Plaintiff Burns is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Burns diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her Plaintiff Burns uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

139. Plaintiff Burns only allowed Defendant to maintain, store, and use her Private

Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

140. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Burns suffered injury from a loss of privacy.

141. Plaintiff Burns has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff Burns was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

142. Upon information and belief, Plaintiff's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft so far in the form of fraudulent charges to her Chase Bank debit card. Specifically, on November 13, 2023, Plaintiff Burns received a text message from Chase informing her that her card had been "compromised" due to fraudulent charges to her account. Chase immediately closed her account, sent her a new card, and opened a new checking account on her behalf. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

143. Furthermore, Plaintiff Burns has experienced daily spam calls and text messages as a result of the Data Breach.

144. The Data Breach has also caused Plaintiff Burns to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and

misuse resulting from her Private Information being misused to commit fraud and placed in the hands of criminals.

145. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Burns to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, self-monitoring her accounts and credit reports to ensure no additional fraudulent activity has occurred, and spending hours addressing the compromise of her Chase account. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

146. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Burns to suffer stress, fear, and anxiety.

147. Plaintiff Burns has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Donna Allen's Experience

148. Plaintiff Donna Allen is an adult individual and a natural person residing in Osage Beach, Missouri, where she intends to stay.

149. Plaintiff Allen provided her information to Defendant Navvis indirectly through her medical provider, who, upon information and belief, uses services provided by Defendant.

150. Plaintiff Allen received a notice letter from Defendant Navvis informing her of the Data Breach and the exposure of her Private Information.

151. The notice letter informed Plaintiff Allen that her Private Information, including her name, Bene Hic number, date of birth, diagnosis/clinical information, health insurance policy-related number, medical date of service, medical provider name, and patient account number, was

stolen in the Data Breach.

152. Plaintiff Allen is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Allen stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Allen diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her, Plaintiff Allen uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

153. Plaintiff Allen only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff Allen's Private Information was within the possession and control of Defendant at the time of the Data Breach.

154. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Allen suffered injury from a loss of privacy.

155. Plaintiff Allen has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

156. Upon information and belief, Plaintiff Allen's Private Information has already been stolen and misused as she has received notifications through Experian that her Private Information

has been found listed on the dark web. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Allen's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

157. The Data Breach has also caused Plaintiff Allen to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

158. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Allen has spent significant time reviewing her financial reports and credit reports for any signs of fraud. Furthermore, she has had to review her security settings and change her passwords for her important online and financial accounts.

159. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Allen to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

160. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Allen to suffer stress, fear, and anxiety.

161. Plaintiff Allen has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Duane Zellmer's Experience

162. Plaintiff Duane Zellmer is an adult individual and a natural person residing in Seffner, Florida, where he intends to stay.

163. Plaintiff Zellmer provided his information to Navvis, upon information and belief, indirectly through providing his information to his medical care providers affiliated with the Florida Medical Group.

164. Plaintiff Zellmer received a notice letter from Defendant Navvis informing him of the Data Breach and the exposure of his Private Information.

165. The notice letter informed Plaintiff Zellmer that certain of his Private Information was stolen in the Data Breach, including his name, date of birth, health plan information, medical treatment information, medical record number, patient account number, case identification number, provider and doctor information, and health record information.

166. Plaintiff Zellmer is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Zellmer stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Zellmer diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff Zellmer uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

167. Plaintiff Zellmer only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff Zellmer's Private Information was within the possession and control of Defendant at the time of the Data Breach.

168. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Zellmer suffered injury from a loss of privacy.

169. Plaintiff Zellmer has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff Zellmer was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

170. Upon information and belief, Plaintiff Zellmer's Private Information has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of actual fraudulent charges to his credit card account with Truist throughout the month of December 2023. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Zellmer's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

171. The Data Breach has also caused Plaintiff Zellmer to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being actually misused and placed in the hands of criminals.

172. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Zellmer was forced to spend several hours reporting fraudulent charges to his credit card account and working with Truist bank to cancel the card and reissue a new one. Further, Plaintiff has spent additional time regularly monitoring his accounts and credit reports for other instances of fraud.

173. In addition to the increased risk and the actual harm suffered, the Data Breach has

caused Plaintiff Zellmer to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

174. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Zellmer to suffer stress, fear, and anxiety.

175. Plaintiff Zellmer has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Julie Montiel's Experience

176. Plaintiff Julie Montiel is an adult individual and a natural person residing in Baraboo, Wisconsin, where she intends to stay.

177. Plaintiff Montiel provided her information to Defendant as a result of her and her family's use of a doctor's office which uses a platform or service provided by Navvis.

178. Plaintiff Montiel received a notice letter from Defendant addressed to her as the parent or guardian of her minor child, E.C., informing her of the Data Breach and the exposure of E.C.'s Private Information.

179. The notice letter informed Plaintiff Montiel that her daughter's Private Information, including her name, Bene Hic number, date of birth, diagnosis/clinical information, health insurance policy-related number, medical date of service, medical provider name, medical provider NPI, patient account number, and Subscriber ID, was stolen in the Data Breach.

180. Plaintiff Montiel is a reasonably cautious person and parent and is therefore careful about sharing the sensitive Private Information of her and her family. As a result, she has never

knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Montiel stores any documents containing sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Montiel diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her Plaintiff Montiel uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

181. Plaintiff Montiel only allowed Defendant to maintain, store, and use her and her daughter's Private Information because she believed that Defendant would use basic security measures to protect the Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff Montiel's and E.C.'s Private Information was within the possession and control of Defendant at the time of the Data Breach.

182. In the instant that E.C.'s Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff's child suffered injury from a loss of privacy.

183. E.C. has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Montiel entrusted to Defendant. This information has inherent value that E.C. was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

184. Upon information and belief, Plaintiff Montiel and her daughter's Private Information has already been stolen and misused as Plaintiff Montiel has received reports that both her and her daughter's Private Information has been listed on the dark web. These actions by

unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

185. Furthermore, Plaintiff Montiel has observed a marked increase in spam calls and texts as a result of the Data Breach. Alarmingly, she has received calls from a bank regarding a business account that she never set up.

186. The Data Breach has also caused Plaintiff Montiel to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her and her daughter's Private Information being placed in the hands of criminals.

187. As a result of the actual harm suffered and the increased imminent risk of future harm, Plaintiff has spent considerable time trying to mitigate the effects of this Data Breach for both her and her daughter. She has set up a free account with Credit Karma and has been using it persistently to monitor her own credit while also monitoring for any misuse of her daughter's Private Information.

188. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Montiel to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

189. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Montiel to suffer stress, fear, and anxiety both that her own information has been and may continue to be abused by criminals, but also that her daughter, a minor, may be exposed to identity theft and fraud before she even begins her adult life.

190. Plaintiff Montiel has a continuing interest in ensuring that her and her daughter's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Julie Schaus's Experience

191. Plaintiff Julie Schaus is an adult individual and a natural person of Wisconsin, residing in Dane County, where she intends to stay.

192. Plaintiff Schaus provided her information to Defendant as a condition of her being a plan member of one of Defendant's clients.

193. Plaintiff Julie Schaus received a notice letter from Defendant Navvis dated December 29, 2023, informing her of the Data Breach and the exposure of her Private Information.

194. The notice letter informed Plaintiff Schaus that her name, date of birth, diagnosis/clinical information, health insurance policy-related number, medical date of service, medical provider name, medical provider treatment/procedure information, member ID, other patient identifier, patient account number, plan name, and Subscriber ID was stolen in the Data Breach.

195. Plaintiff Schaus is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Schaus stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Schaus diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her, Plaintiff Schaus uses two-factor or multifactor authentication to add an extra layer of security to her Private

Information.

196. Plaintiff Schaus only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

197. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Schaus suffered injury from a loss of privacy.

198. Plaintiff Schaus has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff Schaus was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

199. Upon information and belief, Plaintiff's Personal Information has already been stolen and misused as she has received reports from Experian and McAfee that her Private Information has been disseminated across the dark web. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

200. Furthermore, Plaintiff Schaus has experienced an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

201. The Data Breach has also caused Plaintiff Schaus to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

202. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Schaus made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach to verify the incident and obtain more details on its occurrence, contacting McAfee to ensure her accounts are secure, paying approximately $160 to obtain increased security protection services from McAfee, placing credit freezes and placing holds on her accounts through credit bureaus, and placing filters on her email in response to an increase in spam emails. Plaintiff has spent significant time and money remedying the breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

203. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Schaus to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

204. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Schaus to suffer stress, fear, and anxiety which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

205. Plaintiff Schaus has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Kelley Bogart's Experience

206. Plaintiff Keeley Bogart is an adult individual and a natural person of Illinois, residing in Madison County, where she intends to stay.

207. Plaintiff Bogart provided her information to Navvis as a condition of receiving services at SSM Health, which, upon information and belief, contracted with Defendant for services.

208. Plaintiff Bogart received a notice letter from Defendant dated December 29, 2023, informing her of the Data Breach and the exposure of her Private Information.

209. The notice letter informed Plaintiff Bogart that her name, date of birth, diagnosis/clinical information, health insurance policy-related number, medical date of service, medical provider name, medical provider treatment/procedure information, member ID, other patient identifier, patient account number, plan name, and Subscriber ID was stolen in the Data Breach.

210. Plaintiff Bogart is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Bogart stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Bogart diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her Plaintiff Bogart uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

211. Plaintiff Bogart only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff Bogart's Private Information was

within the possession and control of Defendant at the time of the Data Breach.

212. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Bogart suffered injury from a loss of privacy.

213. Plaintiff Bogart has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Bogart entrusted to Defendant. This information has inherent value that Plaintiff Bogart was deprived of when her Private Information was placed on a publicly accessible database and exfiltrated by cybercriminals.

214. Furthermore, Plaintiff Bogart has experienced an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

215. The Data Breach has also caused Plaintiff Bogart to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

216. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Bogart made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach to verify the incident and obtain more details on its occurrence, contacting Defendant to obtain more details on the Data Breach's occurrence, and monitoring her credit score. Plaintiff Bogart has spent significant time remedying the breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

217. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Bogart to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time,

which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

218. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Bogart to suffer stress, fear, and anxiety which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

219. Plaintiff Bogart has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Richard Lilly's Experience

220. Plaintiff Richard Lilly is an adult individual and a natural person of Missouri, residing in Cole County, where he intends to stay.

221. Plaintiff Lilly provided his information to Defendant only indirectly, as part of medical services received at SSM Hospitals.

222. Plaintiff Richard Lilly received a notice letter from Defendant dated December 29, 2023, informing him of the Data Breach and the exposure of his Private Information.

223. The notice letter informed Plaintiff Lilly that his name, date of birth, social security number, and medical information was stolen in the Data Breach.

224. Plaintiff Lilly is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Lilly stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Lilly diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him, Plaintiff Lilly uses two-factor

or multifactor authentication to add an extra layer of security to his Private Information.

225. Plaintiff Lilly only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff Lilly's Private Information was within the possession and control of Defendant at the time of the Data Breach.

226. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Lilly suffered injury from a loss of privacy.

227. Plaintiff Lilly has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff Lilly entrusted to Defendant. This information has inherent value that Plaintiff Lilly was deprived of when his Private Information was placed on a publicly accessible database and exfiltrated by cybercriminals.

228. Furthermore, Plaintiff Lilly has experienced increased spam texts and emails containing his personal information as a result of the Data Breach.

229. The Data Breach has also caused Plaintiff Lilly to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

230. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Lilly incurred additional expenses in the form of time lost monitoring credit and bank statements and the cost of services including dark web monitoring from his credit card company.

231. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Lilly to spend significant time dealing with issues related to the Data Breach,

which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

232. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Lilly to suffer stress, fear, and anxiety.

233. Plaintiff Lilly has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Jeff Ruderman's Experience

234. Plaintiff Jeff Ruderman is an adult individual and a natural person residing in Livingston, New Jersey, where he intends to stay.

235. Plaintiff Ruderman provided his information to Defendant Navvis indirectly through his medical provider, who, upon information and belief, uses services provided by Defendant.

236. Plaintiff Ruderman received a notice letter from Defendant Navvis informing him of the Data Breach and the exposure of his Private Information.

237. Plaintiff Ruderman did not receive a notice letter from Defendant until on or around February 9, 2024.

238. The notice letter informed Plaintiff Ruderman that his Private Information, including his name, date of birth, health plan information, medical treatment information, medical record number, patient account number, case identification number, provider and doctor information, and health record information, was stolen in the Data Breach.

239. Plaintiff Ruderman is a reasonably cautious person and is therefore careful about

sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Ruderman stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him, Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

240. Plaintiff Ruderman only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff Ruderman's Private Information was within the possession and control of Defendant at the time of the Data Breach.

241. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Ruderman suffered injury from a loss of privacy.

242. Plaintiff Ruderman has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff Ruderman entrusted to Defendant. This information has inherent value that Plaintiff Ruderman was deprived of when his Private Information was placed on a publicly accessible database and exfiltrated by cybercriminals.

243. The Data Breach has caused Plaintiff Ruderman to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

244. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Ruderman has spent significant time reviewing his financial accounts and credit reports for any signs of fraud.

245. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Ruderman to spend significant time and money dealing with issues related to the Data Breach, which includes purchasing identity theft insurance for $20 a month, time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

246. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Ruderman to suffer stress, fear, and anxiety.

247. Plaintiff Ruderman has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches

V. CLASS ACTION ALLEGATIONS

248. Plaintiffs bring this class action on behalf of themselves, a Nationwide Class (the "Class"), and certain State Subclasses, including a Florida Subclass, Wisconsin Subclass, Illinois Subclass, and New Jersey Subclass pursuant to Federal Rules of Civil Procedure, Rules 23(b)(2), 23(b)(3), and 23(c)(4).

249. The nationwide Class that Plaintiffs seek to represent is defined as follows:

Nationwide Class:

All persons residing in the United States whose Private Information was compromised during the Data Breach that is the subject of the Notice of Data Breach published by Defendant on or about December 29, 2023 or February 9, 2024 (the "Class", or "Class Members").

250. The State Subclasses are defined as follows:

Florida Subclass:

All persons residing in the State of Florida whose Private Information was compromised during the Data Breach that is the subject of the Notice of Data Breach published by Defendant on or about December 29, 2023 or February 9, 2024.

Wisconsin Subclass:

All persons residing in the State of Wisconsin whose Private Information was compromised during the Data Breach that is the subject of the Notice of Data Breach published by Defendant on or about December 29, 2023 or February 9, 2024.

Illinois Subclass:

All persons residing in the State of Illinois whose Private Information was compromised during the Data Breach that is the subject of the Notice of Data Breach published by Defendant on or about December 29, 2023 or February 9, 2024.

New Jersey Subclass:

All persons residing in the State of New Jersey whose Private Information was compromised during the Data Breach that is the subject of the Notice of Data Breach published by Defendant on or about December 29, 2023 or February 9, 2024.

251. Excluded from the Class are: (i) Defendant and its employees, officers, directors, affiliates, parents, subsidiaries, and any entity in which Defendant has a whole or partial ownership of financial interest; (ii) all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; (iii) any counsel and their respective staff appearing in this matter; and (iv) all judges assigned to hear any aspect of this litigation, their immediate family members, and their respective court staff.

252. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

253. **Numerosity**. The Class is so numerous that joinder of all members is impracticable.

The Class includes thousands of individuals whose personal data was compromised by the Data Breach. The exact number of Class members is in the possession and control of Defendant and will be ascertainable through discovery. But, upon information and belief, the number of affected individuals exceeds 1,000.

254. **Commonality.** There are numerous questions of law and fact common to Plaintiffs and the Class that predominate over any questions that may affect only individual Class Members, including, without limitation:

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

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

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

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

f. Whether Defendant breached duties to Plaintiffs and Class Members to safeguard their Private Information;

g. Whether cyber criminals obtained Plaintiffs' and Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and

monitoring processes were deficient;

i. Whether Defendant owed a duty to provide Plaintiffs and Class Members timely notice of this Data Breach, and whether Defendant breached that duty;

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

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct violated federal law;

m. Whether Defendant's conduct violated state law; and

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

255. **Typicality**. Plaintiffs' claims are atypical of the claims of the Class in that Plaintiffs, like all proposed Class Members, had her Private Information compromised, breached, or otherwise stolen in the Data Breach. Plaintiffs and the Class were injured through the uniform misconduct of Defendant, described throughout this Complaint, and assert the same claims for relief.

256. **Adequacy**. Plaintiffs and counsel will fairly and adequately protect the interests of Plaintiffs and the proposed Class. Plaintiffs retained counsel who are experienced in class action and complex litigation, particularly cases such as this case involving a data breach. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of other Class Members.

257. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would

therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiffs and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiffs know of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

258. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

259. Class certification, therefore, is appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

260. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification

because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed its legal duty or obligation to Plaintiffs and the Class to exercise due care in collecting, storing, using, safeguarding, or otherwise maintaining their Private Information;

b. Whether Defendant breached its legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, using, safeguarding, or otherwise maintaining their Private Information;

c. Whether Defendant failed to comply with its own policies or procedures and applicable laws, regulations, and industry standards relating to data security;

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

e. Whether Plaintiffs and the Class are entitled to actual damages, credit monitoring, or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

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

261. Plaintiffs and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

262. Plaintiffs and the Class entrusted Defendant with their Private Information.

263. Plaintiffs and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and not disclose their Private Information to unauthorized third parties.

264. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, using, maintaining, and protecting their Private Information from unauthorized third parties.

265. The legal duties owed by Defendant to Plaintiffs and the Class include, but are not limited to the following:

a. To exercise reasonable care in procuring, retaining, securing, safeguarding, deleting, and protecting the Private Information of Plaintiffs and the Class in Defendant's possession;

b. To protect Private Information of Plaintiffs and the Class in Defendant's possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes and software to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Class of the Data Breach.

266. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use

reasonable measures to protect Private Information.

267. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiffs and Class Members are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and by not complying with industry standards.

268. Defendant breached its duties to the Plaintiffs and the Class. Defendant knew or should have known the risks of collecting and storing Private Information and the importance of maintaining secure systems, especially in light of the fact that data breaches have recently been prevalent.

269. Defendant knew or should have known that its security practices did not adequately safeguard the Private Information of Plaintiffs and the Class.

270. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security measures and its failure to protect the Private Information of Plaintiffs and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and the Class during the period it was within Defendant's possession and control.

271. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

272. Defendant was subject to an "independent duty" to Plaintiffs and the Class.

273. Defendant's own conduct created a foreseeable risk of harm to an individual,

including Plaintiffs and the Class. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for safekeeping the Private Information of Plaintiffs and the Class, including basic encryption techniques freely available to Defendant.

274. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

275. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiffs and the Class.

276. Defendant breached the duties it owes to Plaintiffs and the Class in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs and the Class's Private Information and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that its systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to Plaintiffs and the Class that their Private Information had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

277. There is a close causal connection between Defendant's failure to implement

security measures to protect the Private Information of Plaintiffs and Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was stolen and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

278. The Private Information taken in the Data Breach can (and already has been) used for identity theft and other types of financial fraud against Plaintiffs and the Class.

279. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year. To date, Defendant has only offered twelve (12) months of complimentary credit-monitoring services.

280. As a result of Defendant's negligence, Plaintiffs and the Class suffered injuries that include:

i. the lost or diminished value of Private Information;

ii. actual misuse in the forms of identity theft and financial fraud;

iii. the dissemination of Plaintiffs' and Class Members' Private Information to the dark web;

iv. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;

v. lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards

believed to be associated with the compromised account;

vi. the continued risk to their Private Information, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession;

vii. future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and the Class, including ongoing credit monitoring.

281. These injuries were reasonably foreseeable given the history and uptick of data security breaches of this nature within the medical sector. The injury and harm that Plaintiffs and the Class suffered was the direct and proximate result of Defendant's negligent conduct.

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

282. Plaintiffs and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

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

284. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures

to protect Private Information and comply with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored.

285. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.304, 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).

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

287. Plaintiffs and the Class are within the class of persons that the FTCA and HIPAA were intended to protect.

288. The harm that occurred as a result of the Data Breach is the type of harm the FTCA and HIPAA were intended to guard against. The FTC has pursued enforcement actions against businesses, which have failed to employ reasonable data security measures and avoid unfair and deceptive practices, causing the same harm as that suffered by Plaintiffs and the Class.

289. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual instances of identity theft or fraud; (ii) the compromise, publication, and/or theft of their Private Information, which has already been found on the dark web; (iii) out-of-pocket expenses associated with the

prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud, identity theft, and/or other various forms of fraud (v) costs associated with placing or removing freezes on credit reports; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and the Class in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

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

291. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Class)

292. Plaintiffs and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

293. This Count is pleaded in the alternative to the breach of implied contract and breach of third-party beneficiary contract claims below.

294. Plaintiffs and the Class conferred a monetary benefit to Defendant by providing Defendant with their valuable Private Information, which Defendant knowingly used or retained in the course of its business.

295. Defendant benefited from receiving Plaintiffs' and the Class Members' Private Information by its ability to retain and use that information for its own financial benefit. Defendant understood this benefit and accepted the benefit knowingly.

296. Defendant also understood and appreciated that the Private Information of Plaintiffs and the Class was private and confidential to them, and that its value depended upon Defendant maintaining the privacy and confidentiality of that Private Information.

297. Plaintiffs and the Class conferred a monetary benefit upon Defendant in the form of monies paid to Defendant for services.

298. The monies paid to Defendant for services were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

299. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiffs and the Class by utilizing cheaper, ineffective security measures. Plaintiffs and the Class, on the other hand, suffered a direct and proximate result of Defendant's failure to provide the requisite security.

300. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that Private Information would not have been transferred to and entrusted with Defendant. Indeed, if Defendant had informed its customers that Defendant's data and cyber

security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

301. As a result of Defendant's wrongful conduct, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class. Defendant continues to benefit and profit from its retention and use of Plaintiffs' and Class Members' Private Information while its value to Plaintiffs and the Class has been diminished.

302. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including compiling, using, and retaining Plaintiffs' and the Class's Private Information, while at the same time failing to maintain that information securely from intrusion and theft by cyber criminals, hackers, and identity thieves.

303. Plaintiffs and the Class have no adequate remedy at law.

304. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and the Class paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

305. Defendant acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

306. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and the Class, proceeds that it unjustly received from them.

307. As a direct and proximate result of Defendant's below-described breach of implied

contract and breach of third-party beneficiary contract, Plaintiffs and the Class have suffered, and will continue to suffer an ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identify theft crimes, fraud, and abuse resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic time that the Plaintiffs and the Class have not been compensated for.

308. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm.

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

309. Plaintiffs and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

310. Plaintiffs and the Class entrusted their Private Information with Defendant. In doing so, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached, compromised, or stolen.

311. The statements in Defendant's Privacy Policy described herein support the existence of an implied contract. Specifically, Defendant's privacy policy "recognizes that the privacy

of…personal information is important…"[18] As such, Defendant promised to only share Private Information with "third parties who perform functions or services on [Navvis's] behalf as outlined in this Privacy Policy and otherwise as permitted by law."[19]

312. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

313. Defendant breached the implied contracts with Plaintiffs and the Class by failing to safeguard and protect their Private Information, by failing to delete the Private Information of Plaintiffs and the Class once their relationship ended, and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the Data Breach.

314. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class have suffered, and will continue to suffer, ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identify theft crimes, fraud, and abuse resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic time that the Plaintiffs and the Class have not been compensated for.

315. As a direct and proximate result of the Defendant's above-described breach of implied contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal

---

18 https://www.navvishealthcare.com/legal/#:~:text=We%20collect%20and%20may%20use,services%20and%20to%20improve%20the

19 *Id.*

damages.

COUNT V
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiffs and the Class)

316. Plaintiffs and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

317. Upon information and belief, Defendant entered into virtually identical contracts with its clients to provide healthcare support services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

318. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties, and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

319. Defendant knew that if it were to breach these contracts with its clients, Plaintiffs and the Class would be harmed.

320. Defendant breached its contracts with its clients and, as a result, Plaintiffs and Class Members were affected by this Data Breach when Defendant failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

321. As foreseen, Plaintiffs and the Class were harmed by Defendant's failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the theft of their Private Information.

322. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

COUNT VI
INVASION OF PRIVACY
(On behalf of Plaintiffs and the Class)

323. Plaintiffs and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

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

325. As a result of Defendant's intentional failure to employ adequate data security measures, publicity was given to Plaintiffs' and Class Members' Private Information, which necessarily includes matters concerning their private life.

326. A reasonable person of ordinary sensibilities would consider the publication of Plaintiffs' and Class Members' Private Information to be highly offensive.

327. Plaintiffs' and Class Members' Private Information is not of legitimate public concern and should remain private.

328. As a direct and proximate result of Defendant's intentional public disclosure of private facts, Plaintiffs and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft

monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

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

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

COUNT VII
BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiffs and the Class)

331. Plaintiffs and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

332. Every contract in this state has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached, even when there is no breach of a contract's express terms.

333. In addition, there exists an implied covenant of good faith and fair dealing in all contracts that neither party shall do anything that will have the effect of destroying or injuring the right of the other party to receive the fruits of the contract. 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.

Evading the spirit of the bargain and abusing the power to specify terms constitute examples of bad faith in the performance of contracts.

334. 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. Examples of bad faith are evasion of the spirit of the bargain, willful rendering of imperfect performance, abuse of a power to specify terms, and interference with or failure to cooperate in the other party's performance.

335. Plaintiffs and the Class have complied with and performed all conditions of their contracts with Defendant.

336. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members, and the continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of its security vulnerabilities of the systems that were exploited in the Data Breach.

337. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT VIII
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On behalf of Plaintiffs and the Class)

338. Plaintiffs and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

339. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C.

§ 2201.

340. Defendant owes a duty of care to Plaintiffs and the Class that requires it to adequately secure Plaintiffs' and the Class's Private Information.

341. Defendant failed to fulfill their duty of care to safeguard Plaintiffs' and the Class's Private Information.

342. Plaintiffs and the Class are at risk of harm due to the exposure of their Private Information and Defendant's failure to address the security failings that lead to such exposure.

343. Plaintiffs, therefore, seek a declaration that (1) Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with its explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its user applications by, among other things, creating

firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiffs and the Class for a period of ten years; and

h. Meaningfully educating Plaintiffs and the Class about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

COUNT IX
VIOLATIONS OF FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. § 501.201, *et seq*. ("FDUTPA")
(On behalf of Plaintiff Zellmer and the Florida Subclass)

344. Plaintiff Duane Zellmer and the Florida Subclass re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

345. Plaintiff Zellmer brings this claim, individually and on behalf of the Florida Subclass, against Defendant for violations of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, et seq. ("FDUTPA").

346. Defendant engaged in unfair or deceptive acts or practices in the conduct of its trade or commerce, in violation of the FDUTPA, Fla. Stat. § 501.204, by, among other things, omitting and concealing the material fact that Defendant did not implement and maintain adequate data

security measures to secure consumers' Private Information and by making implied or implicit representations that its data security practices were sufficient to protect consumers' Private Information.

347. Defendant's deceptive, unfair, and unlawful acts or practices in violation of the FDUTPA include:

a. Implementing inadequate data security and privacy measures to protect Plaintiff Zellmer's and Florida Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Zellmer's and Florida Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Zellmer's and Florida Subclass Members' Private Information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Zellmer's and Florida Subclass Members' Private Information, including duties imposed by the

Federal Trade Commission Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Zellmer's and Florida Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Zellmer's and Florida Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

348. Defendant's representations and omissions were material because they were likely to and did deceive reasonable consumers, including Plaintiff Zellmer and Florida Subclass Members, about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

349. Defendant intended to mislead Plaintiff Zellmer and Florida Subclass Members and induce them to rely on their misrepresentations and omissions.

350. Past breaches in the medical services industry put Defendant on notice that its data security practices were inadequate to safeguard Plaintiff Zellmer's and Florida Subclass Members' Private Information, and Defendant knew or should have known that the risk of a data breach was highly likely.

351. Plaintiff Zellmer and Florida Subclass Members reasonably expected that Defendant's data security, digital platforms, and data storage systems were adequately secure to protect their Private Information.

352. Plaintiff Zellmer and Florida Subclass Members relied on Defendant to advise

customers if their data security, digital platforms, and data storage systems were not adequately secure to protect their Private Information.

353. Plaintiff Zellmer and Florida Subclass Members had no opportunity to make any inspection of Defendant's data security practices or to otherwise ascertain the truthfulness of Defendant's representations and omissions regarding data security, including Defendant's failure to alert customers that its data security, digital platforms, and data storage systems were not adequately secure and, thus, were vulnerable to attack.

354. Plaintiff Zellmer and Florida Subclass Members relied to their detriment on Defendant's misrepresentations and deceptive omissions regarding their data security practices.

355. Had Defendant disclosed to Plaintiff Zellmer and Florida Subclass Members that their data security, digital platforms, and data storage systems were not secure, and thus, vulnerable to attack, Plaintiff Zellmer and Florida Subclass Members would not have entrusted Defendant with their Private Information, and Defendant would have been forced to comply with the law and adopt reasonable data security measures or would have been unable to continue in business.

356. As a direct and proximate result of Defendant's unfair and deceptive business practices, Plaintiff Zellmer and Florida Subclass Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach, the lost value of their Private Information, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

357. Plaintiff Zellmer and the Florida Subclass seek all monetary and non-monetary relief allowed by law.

COUNT X
VIOLATIONS OF WISCONSIN DECEPTIVE TRADE PRACTICES ACT
Wis. Stat. Ann. § 100.18, *et seq*. ("Wisconsin DTPA")
(On behalf of Plaintiff Julie Montiel, on behalf of her minor child, E.C., Plaintiff Julie Schaus, and the Wisconsin Subclass)

358. Plaintiff Julie Montiel, on behalf of her minor child, E.C., Plaintiff Julie Schaus, and the Wisconsin Subclass (collectively, "Wisconsin Plaintiffs") re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

359. The Wisconsin Plaintiffs bring their claim against Defendant for violation of the Wisconsin Deceptive Trade Practices Act, Wis. Stat. § 100.18(1) ("Wisconsin DTPA"), which prohibits untrue, deceptive, or misleading representations in the sale of goods and services to consumers.

360. Defendant is a "corporation[s] or association[s]," as defined by the Wisconsin DTPA, Wis. Stat. § 100.18(1).

361. The Wisconsin Plaintiffs are members of "the public," as defined by the Wisconsin DTPA, Wis. Stat. § 100.18(1).

362. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Defendant to members of the public for sale, use, or distribution, Defendant made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of the Wisconsin DTPA, Wis. Stat. § 100.18(1).

363. Defendant also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as

advertised, in violation of the Wisconsin DTPA, Wis. Stat. § 100.18(9).

364. Defendant's deceptive acts, practices, plans, and schemes in violation of the Wisconsin DTPA include:

a. Implementing inadequate data security and privacy measures to protect the Private Information of the Wisconsin Plaintiffs, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures, despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Private Information of the Wisconsin Plaintiffs, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of the Private Information of the Wisconsin Plaintiffs, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of the Private Information of the Wisconsin Plaintiffs, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure the Private Information of the Wisconsin

Plaintiffs; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of the Private Information of the Wisconsin Plaintiffs, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

365. Defendant intended to mislead the Wisconsin Plaintiffs and induce them to rely on their misrepresentations and omissions.

366. Defendant's representations and omissions were material because they were likely to and did deceive reasonable consumers, including the Wisconsin Plaintiffs, about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

367. Defendant had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity of the Private Information in its possession, and the generally accepted professional standards in the medical services industry. This duty arose because members of the public, including the Wisconsin Plaintiffs, repose a trust and confidence in Defendant. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including the Wisconsin Plaintiffs—and Defendant, because consumers are unable to fully protect their interests with regard to their data and placed trust and confidence in Defendant. Defendant's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the inadequate security of the data in their systems;

b. Active concealment of the inadequate condition of their data security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems.

368. Because the above facts are material to a reasonable person in the Wisconsin Plaintiffs' position, the law treats Defendant's failure to disclose them as being identical to actively representing that those facts do not exist.

369. Defendant acted intentionally, knowingly, and maliciously to violate the Wisconsin DTPA, and recklessly disregarded the rights of the Wisconsin Plaintiffs.

370. As a direct and proximate result of Defendant's unfair and deceptive acts or practices, the Wisconsin Plaintiffs have suffered and will continue to suffer ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; a substantially increased and imminent risk of fraud and identity theft; loss of value of their Private Information, and the need to dedicate future expenses and time to protect themselves against further loss.

371. Defendant had an ongoing duty to the Wisconsin Plaintiffs to refrain from deceptive acts, practices, plans, and schemes under the Wisconsin DTPA, Wis. Stat. § 100.18. 660. The Wisconsin Plaintiffs seek all monetary and nonmonetary relief allowed by law.

COUNT XI
VIOLATIONS OF ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
815 Ill. Comp. Stat. §§ 510, *et seq*. ("Illinois DTPA")
(On behalf of Plaintiff Keeley Bogart and the Illinois Subclass)

372. Plaintiff Keeley Bogart and the Illinois Subclass re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

373. Plaintiff Bogart brings this claim, individually and on behalf of the Illinois

Subclass, against Defendant for violations of the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. §§ 510, et seq. ("Illinois DTPA").

374. Defendant is a "person[s]" as defined by the Illinois DTPA, 815 Ill. Comp. Stat. § 510/1(5).

375. Defendant engaged in deceptive trade practices in the conduct of their business, in violation of the Illinois DTPA, 815 Ill. Comp. Stat. §§ 510/2, which prohibits companies like Defendant from:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in any other conduct that creates a likelihood of confusion or misunderstanding.

376. Defendant engaged in unfair and deceptive acts and practices in violation of the Illinois DTPA, 815 Ill. Comp. Stat. §§ 510/2(a)(5), (7), (9) and (12), by, among other things, omitting and concealing the material fact that Defendant did not implement and maintain adequate data security measures to secure consumers' Private Information and by making implied or implicit representations that its data security practices were sufficient to protect consumers' Private Information.

377. Defendant's deceptive, unfair, and unlawful acts or practices in violation of the Illinois DTPA include:

a. Implementing inadequate data security and privacy measures to protect

Plaintiff Bogart's and Illinois Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bogart's and Illinois Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Bogart's and Illinois Subclass Members' Private Information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bogart's and Illinois Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Bogart's and Illinois Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and

privacy of Plaintiff Bogart's and Illinois Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

378. Defendant's representations and omissions were material because they were likely to and did deceive reasonable consumers, including Plaintiff Bogart and Illinois Subclass Members, about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

379. Defendant intended to mislead Plaintiff Bogart and Illinois Subclass Members and induce them to rely on their misrepresentations and omissions.

380. Past breaches in the medical services industry put Defendant on notice that its data security practices were inadequate to safeguard Plaintiff Bogart's and Illinois Subclass Members' Private Information, and Defendant knew or should have known that the risk of a data breach was highly unlikely.

381. Plaintiff Bogart and Illinois Subclass Members reasonably expected that Defendant's data security, digital platforms, and data storage systems were adequately secure to protect their Private Information.

382. Plaintiff Bogart and Illinois Subclass Members relied on Defendant to advise customers if its data security, digital platforms, and data storage systems were not adequately secure to protect their Private Information.

383. Plaintiff Bogart and Illinois Subclass Members had no opportunity to make any inspection of Defendant's data security practices or to otherwise ascertain the truthfulness of Defendant's representations and omissions regarding data security, including Defendant's failure to alert customers that its data security, digital platforms, and data storage systems were not

adequately secure and, thus, were vulnerable to attack.

384. Plaintiff Bogart and Illinois Subclass Members relied to their detriment on Defendant's misrepresentations and deceptive omissions regarding data security practices.

385. Had Defendant disclosed to Plaintiff Bogart and Illinois Subclass Members that its data security, digital platforms, and data storage systems were not secure, and thus, vulnerable to attack, Plaintiff Bogart and Illinois Subclass Members would not have entrusted Defendant with their Private Information, and Defendant would have been forced to comply with the law and adopt reasonable data security measures or would have been unable to continue in business.

386. As a direct and proximate result of Defendant's unfair and deceptive business practices, Plaintiff Bogart and Illinois Subclass Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the lost value of their Private Information, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

387. Plaintiff Bogart and the Illinois Subclass seek all monetary and non-monetary relief allowed by law.

COUNT XII
VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT
N.J. Stat. Ann. § 56:8-1 et seq. ("NJ CFA")
(On behalf of Plaintiff Jeff Ruderman and the New Jersey Subclass)

388. Plaintiff Jeff Ruderman and the New Jersey Subclass re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

389. The deceptive and misleading statements and representations set forth above are

advertisements within the meaning of N.J. Stat. Ann. § 56:8-1(a).

390. Defendant is a "person" within the meaning of N.J. Stat. Ann. § 56:8-1(d).

391. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, et seq., prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

392. Defendant's unconscionable and deceptive practices include:

a. Implementing inadequate data security and privacy measures to protect Plaintiff Ruderman's and New Jersey Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Ruderman's and New Jersey Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Ruderman's and New Jersey Subclass Members' Private Information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Ruderman's and New Jersey Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Ruderman's and New Jersey Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Ruderman's and New Jersey Subclass Members' Private Information, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

393. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

394. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff Ruderman and the New Jersey Subclass Members, that their Private Information would not be exposed and misled Plaintiff Ruderman and the New Jersey Subclass Members into believing they did not need to take actions to secure their identities.

395. Defendant intended to mislead Plaintiff Ruderman and the New Jersey Subclass Members and induce them to rely on their misrepresentations and omissions.

396. Defendant acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff Ruderman's and New Jersey Subclass Members' rights.

397. As a direct and proximate result of Defendant's unconscionable and deceptive practices, Plaintiff Ruderman and the New Jersey Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; the expense of purchasing multi-year identify theft protection; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

398. Plaintiff Ruderman and the New Jersey Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, request judgment against Defendant and that the Court grant the following:

1. An order certifying the Class and appointing Plaintiffs and their counsel to represent the Class;
2. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the Private Information belonging to Plaintiffs and the Class;
3. Injunctive relief requiring Defendant to:
    a. Engage third-party security auditors/penetration testers as well as

internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engage third-party security auditors and internal personnel to run automated security monitoring;

c. Audit, test, and train its security personnel regarding any new or modified procedures;

d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conduct regular database scanning and security checks;

f. Routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchase credit monitoring services for Plaintiffs and the Class for a period of ten years; and

h. Meaningfully educate Plaintiffs and the Class about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

4. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiffs and all Class Members;

5. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

6. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

7. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

8. Any and all such other and further relief as this Court may deem just and proper.

VI. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand this matter be tried before a jury.

Respectfully submitted,

Dated: March 11, 2024

/s/ Tiffany Marko Yiatras

Tiffany Marko Yiatras
Francis J. "Casey" Flynn, Jr.
CONSUMER PROTECTION LEGAL, LLC
308 Hutchinson Road
Ellisville, Missouri 63011-2029
Tele: 314-541-0317
Tiffany@consumerprotectionlegal.com
casey@consumerprotectionlegal.com

Bryan Bleichner
Philip Krzeski
CHESTNUT CAMBRONNE
100 Washington Ave South. Minneapolis, MN 55401
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Joseph M. Lyon*
Kevin M. Cox*
THE LYON FIRM
2754 Erie Ave. Cincinnati, OH 45208
Phone: (513) 381-2333

jlyon@thelyonfirm.com
kcox@thelyonfirm.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
-and-
212 W. Spring Valley Road
Richardson, TX 75081
wbf@federmanlaw.com

Coordinating Counsel for Plaintiffs

Brandon J.B. Boulware, #54150(MO)
Jeremy M. Suhr, #60075(MO)
BOULWARE LAW LLC
1600 Genessee, Suite 416 Kansas City, MO
64102 Tel: (816) 492-2826
brandon@boulware-law.com
jeremy@boulware-law.com

Mason A. Barney*
Tyler J. Bean
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500 New York,
New York 10151 Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

Terence R. Coates*
Spencer D. Campbell*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530 Cincinnati,
OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
scampbell@msdlegal.com

Laura Van Note (E.D. Mo Bar # 310160CA)
COLE & VAN NOTE
555 12th St., Ste. 2100
Oakland, CA 94607

Telephone: (510) 891-9800
Facsimile: (510) 891-7030
lvn@colevannote.com

Howard T. Longman
Longman Law, P.C.
354 Eisenhower Parkway, Suite 1800
Livingston, N.J. 07039
Telephone: (973) 994-2315
Facsimile: (973) 994-2319
Hlongman@longman.law

Attorneys for Plaintiffs and Putative Class
**Pro Hac Vice forthcoming*