IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA

KIMBERLY SANDVIG, as an individual and on behalf of all others similarly situated, Plaintiff, v. EYE CARE LEADERS HOLDINGS, LLC, Defendant.	CASE NO.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Kimberly Sandvig ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant Eye Care Leaders Holdings, LLC ("Eye Care Leaders" or "Defendant"), a North Carolina Limited Liability Company, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of the recent targeted data breach of the computer network for Eye Care Leaders, a healthcare software service provider, whereby an unauthorized third-party accessed Defendant's insufficiently secured computer network and exfiltrated a wealth of unencrypted data, including the removal of the highly sensitive personal information and medical records of approximately 342,000 individuals, including approximately 54,000 current and former patients and employees of Summit Eye Associates, P.C. (the "Data Breach"), the eye care clinic used by Plaintiff.

2. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of loss of the value of their private and confidential information, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

3. Plaintiff brings this suit on her own behalf and for similarly situated individuals whose sensitive personal information was entrusted to Defendant's officials and agents, then compromised, unlawfully accessed, and stolen during the Data Breach (collectively "Class Members"). Information compromised in the Data Breach includes individuals' full name, Social Security number, and other personally identifiable information ("PII"), as well as information related to medical record number, information regarding care received at Summit Eye Associates ("Summit Eye") and numerous other eye care clinics, and/or health insurance information, considered protected health information as defined by the HIPAA ("PHI"), all of which Defendant collected and retained on its network (collectively the "Private Information").

4. Plaintiff brings this class action lawsuit on behalf of herself and those similarly situated to address: 1) Defendant's inadequate safeguarding of Class Members' Private Information, 2) Defendant's failure to provide timely and adequate notice to Plaintiff and other Class Members that their Private Information was subject of this Data Breach, and 3) Defendant's failure to notify Plaintiff and Class Members precisely what specific Private Information was accessed and exfiltrated.

5. Defendant maintained Plaintiff's and Class Members' Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition that left it vulnerable to cyberattacks and the exfiltration of Plaintiff's and Class Members' Private Information, as actually happened in this Data Breach.

6. Upon information and belief, this Data Breach and the potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known and foreseeable risk to Defendant, and thus Defendant was on notice that if it failed to take steps necessary to secure its patients' and employees' Private Information (as it did), the PII and PHI would be a dangerous condition and at risk of being stolen.

7. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed patients' Private Information to permit the prompt discovery of the intrusion and reduce the damage suffered by the Class Members.

8. Because of the Data Breach, Plaintiff's and Class Members' Private Information was accessed and exfiltrated by cybercriminals, and upon information and belief, Defendant's systems were not fully operable during its investigation of the Data Breach, resulting in a disruption of its access to Plaintiff's and Class Members' medical records, risking impediments to certain patients' healthcare.

9. In addition, Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves and potentially being sold on the dark web.

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

information to police during an arrest.

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

12. Plaintiff and Class Members have and may incur out of pocket costs in the future when they pay for, among other things, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. In addition, as a direct and proximate result of the Data Breach and subsequent exfiltration of their Personal Information, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges, putting alerts on their credit files, and dealing with spam messages and e-mails received as a result of the Data Breach.

14. Plaintiff and Class Members have likewise suffered and will continue to suffer an invasion of their property interest in their own Private Information such that they are entitled to damages for unauthorized access to, theft of, and misuse of their Private Information from Defendant.

15. Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their Private Information, as thieves are likely to use it to obtain money and credit in Plaintiff's and Class Members' names for years.

16. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or removed from the network during the Data Breach.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages,

reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

18. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct asserting claims for negligence, invasion of privacy, breach of implied contract, breach of fiduciary duty, unjust enrichment

PARTIES

19. Plaintiff Kimberly Sandvig is, and at all times mentioned herein was, an individual citizen of the State of Tennessee. Plaintiff Kimberly Sandvig was a patient at Summit Eye.

20. Defendant Eye Care Leaders Holdings, LLC is a North Carolina Limited Liability Company with its Principal Office at 2222 Sedwick Road, Durham, North Carolina 27713. Eye Care Leaders can be served through its registered manager, Greg E. Lindberg, at 2222 Sedwick Road, Durham, North Carolina 27713.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332, at subsection (d), conferring federal jurisdiction over class actions where, as here: (a) there are 100 or more members in the proposed class; (b) some members of the proposed class have a different citizenship from the citizenship of all of Defendant's members; and (c) the claims of the proposed class members exceed the sum or value of five million dollars ($5,000,000) in aggregate. See 28 U.S.C. § 1332(d)(2) and (6).

22. This Court has personal jurisdiction over Defendant because it has substantial aggregate contacts with this District, including engaging in conduct in this District that has a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout

the United States, and because Defendant purposely availed itself of the laws of the United States and the State of North Carolina.

23. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant is headquartered and has its principal place of business in this District, a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District, and Defendant conducts substantial business in this District.

FACTUAL ALLEGATIONS

Defendant's Business

24. Defendant Eye Care Leaders is a service provider of ophthalmology-specific Electronic Medical Records ("EMR") and Practice Management software systems.

25. Eye Care Leaders is headquartered in Durham, North Carolina.

26. According to Eye Care Leaders' website, Eye Care Leaders services over 9,000 physicians by providing its "comprehensive solutions" and "high-level Analytics and Benchmarking services to meet each practice's needs."[1]

27. Eye Care Leaders provides ophthalmology practice management software and electronic health records systems for 40 percent of the eye care market, bringing together trusted names such as myCare iMedicWare, myCare Integrity EMR, MDoffice, ManagementPlus, Medflow, IO Practiceware, KeyMedical, My Vision Express, and EyeDoc.[2]

28. Summit Eye contracted with Defendant Eye Care Leaders for their myCare Integrity Solution software.

---

[1] *About Eye Care Leaders*, EYE CARE LEADERS, https://eyecareleaders.com/about-eye-care-leaders/ (last accessed June 8, 2022).

[2] *Eye Care Leaders Achieves HITRUST CSF® Certification to Further Mitigate Risk in Third Party Privacy, Security and Compliance*, EYE CARE LEADERS, https://eyecareleaders.com/hitrust-csf-certification/ (last accessed June 8, 2022).

29. myCare Integrity Solution is software for ophthalmic Electronic Medical Records and Practice Management.[3]

30. Additionally, Defendant Eye Care Leaders website states that myCare Integrity Electronic Medical Records software speeds up exams, billing processes, and office workflows, and ensure compliance with federal healthcare laws — without sacrificing quality of patient care.[4]

31. As it conducts its business, Defendant Eye Care Leaders collects highly sensitive patient information from its clients, who collect this information from their patients.

32. More specifically, in ordinary course of receiving medical records from Summit Eye, Defendant Eye Care Leaders was provided (and Plaintiff did in fact provide) with sensitive, personal and private information such as:

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

[3] *Id.*
[4] *Id.*

33. Defendant Eye Care Leaders may also receive private and personal information from other individuals or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patient's health plan(s), close friends, or family members.

34. Even though it claims that it "works in the best interest of eye care practices and ensures operational efficiency, regulatory compliance, and revenue growth," Eye Care Leaders does not follow industry standard practices in securing patient medical records. On information and belief, Eye Care Leaders inadequately trains its employees on cybersecurity policies, fails to enforce those policies, or maintains unreasonable or inadequate security practices and systems.

The Data Breach

35. According to its Notice Letters sent to Plaintiff and Class Members by Summit Eye, on March 1, 2022, Defendant Eye Care Leaders "identified unauthorized access to [its] myCare Integrity data" on or about December 4, 2021.[5] By March 28, 2022 Defendant Eye Care Leaders knew cyberthieves had unauthorized access to and "***deleted databases and system configuration files***" containing patient information from Eye Care Leaders' myCare Integrity network.[6]

36. Defendant Eye Care Leaders began an internal investigation, and informed Summit Eye that that "it does not know whether or not any Summit Eye patient information was involved in the incident" and as a result, it "cannot confirm that any Summit Eye patient information was accessed" and "cannot rule out that possibility."[7]

37. On March 28, 2020, Defendant Eye Care Leaders informed Summit Eye that unauthorized access to patient information may have "included your name, date of birth, medical

[5] *See* Notice Letter, attached as Exhibit A.
[6] *Id.*
[7] *Id.*

record number, health insurance information, Social Security number, and information regarding care received at Summit Eye."[8]

38. Upon information and belief, the cyberattack targeted Defendant due to Defendant's status as a healthcare entity that collects, creates, and maintains PII and PHI. This cyberattack was expressly designed to gain access to private and confidential data, including (among other things) Private Information of patients and employees like Plaintiff and Class Members.

39. Eye Care Leaders stated that upon discovering the Data Breach, Eye Care Leaders' "incident response team immediately stopped the unauthorized access and began investigating the incident."[9]

40. The investigation determined that the files impacted included Plaintiff and Class Members' full name and "one or more of the following: "date of birth, medical record number, health insurance information, Social Security number, and information regarding care received at Summit Eye."[10]

41. Defendant Eye Care Leaders notified Summit Eye on March 1, 2022, nearly 4 months after Eye Care Leaders knew of the Data Breach. *See* Plaintiff's Notice Letter, attached as Exhibit A.

42. The Notice Letters that Summit Eyesent to its patients, informing them of Eye Care Leaders Data Breach, including the Plaintiff and Class Members, are dated April 27, 2022, nearly 5 months after the Eye Care Leaders knew of the Data Breach. *See* Plaintiff's Notice Letter, attached as Exhibit A.

---

[8] *Id.*
[9] *Id.*
[10] *Id.*

43. Despite its lag in notification of the Data Breach that affected patients and employees, Eye Care Leaders offered victims of the attack just 12 months of identity theft services "through IDX, a data breach and recovery services expert, at no charge to patients of Summit Eye affected. These services include 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services."[11]

44. As a consequence of the Data Breach on Defendant's computer systems, highly sensitive and private information belonging to Plaintiff and Class Members that was supposed to be protected by Defendant was removed from Defendant's network

45. Based on the Notice of Data Breach Letters she received, which informed Plaintiff that her Private Information was removed from Defendant's network and computer systems, Plaintiff believes her Private Information was stolen from the Defendant's network (and subsequently sold) in the Data Breach.

46. Further, the removal of the Private Information from Defendant's system – information that included full names, dates of birth, and Social Security numbers (which are the keys to identity theft and fraud) demonstrates that this cyberattack was targeted.

47. Cyberattacks against hospitals and healthcare organizations such as Defendant are targeted. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across US healthcare organizations. Significant security incidents are a near-universal experience in US healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets."[12] "Hospitals have

[11] *Id.*
[12] *HIMMS Healthcare Cybersecurity Survey*, HIMSS, https://www.himss.org/himss-cybersecurity-survey (last accessed June 8, 2022).

emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information (PII) for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[13]

48. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

49. Plaintiff and Class Members provided their Private Information to Summit Eye, who then provided it to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

50. Defendant's data security obligations were particularly important given the substantial increase in data breaches, and particularly data breaches in the healthcare industry, preceding the date of the breach.

51. Data breaches, including those perpetrated against the healthcare sector of the economy, have become widespread.

52. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[14] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[15] The 330

---

[13] Eyal Benishti, How to Safeguard Hospital Data from Email Spoofing Attacks, Chief Healthcare Executive (April 4, 2019) at: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed June 7, 2022).

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

[15] *Id*.

reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[16]

53. Indeed, cyber- attacks, 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.

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

55. 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 Eye Care Leaders.

Defendant Fails to Comply with FTC Guidelines

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

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

[16] *Id.*
[17] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last accessed June 7, 2022).

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

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

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

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

[18] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed June 7, 2022).
[19] *Id.*

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

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

63. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients as outlined in its promise to comply with all federal healthcare laws. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

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

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

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

67. Upon information and belief, 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.

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

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

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

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

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

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

Defendant's Breach

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

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and Data Breaches

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

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

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

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

h. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

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

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

l. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

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

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

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

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

74. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

75. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

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

76. Data Breaches at medical facilities such as Defendant's are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

77. For instance, loss or interruption of access to patient histories, charts, images and other information forces providers to limit or cancel patient treatment because of the disruption of service. Any interruption can lead to a deterioration in the quality of overall care patients receive at facilities affected by Data Breaches and related data breaches.

78. Data Breaches that result in the removal of protected data are also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

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

79. Data breaches represent a significant problem for patients who have already experienced inconvenience and disruption associated with a Data Breach.

80. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone

steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[20]

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

82. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

83. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

84. Theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[21] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

85. Theft of PHI, in particular, is gravely serious: "Medical identity theft is when someone uses your personal information — like your name, Social Security number, health

[20] *See Steps*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last accessed June 8, 2022).

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

insurance account number or Medicare number — to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care. If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[22] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

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

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

88. Where the most private information belonging to Plaintiff and Class Members was accessed and removed from Defendant's network, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

[22] *See* Federal Trade Commission, *Medical Identity Theft*. Available at https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed June 7, 2022).

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

90. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[23] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

91. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[24] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[25] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

92. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he

[23] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed June 7, 2022).
[24] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed June 8, 2022).
[25] *Id.* at 4.

credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[26]

93. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[27]

94. Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is $50 and up.[28]

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

96. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this risk and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

---

[26] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015. Available at http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed June 7, 2022).

[27] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed June 7, 2022).

[28] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last accessed June 7, 2022).

Plaintiff's Experience

97. Plaintiff Kimberly Sandvig is and at all times mentioned herein was an individual citizen residing in the State of Tennessee, in the City of Hermitage, Davidson County.

98. Ms. Sandvig has been a patient of Summit Eye. Summit Eye is a professional Optometrist and Ophthalmologist Corporation in Hermitage, Tennessee. Summit Eye required Ms. Sandvig to provide her Private Information.

99. Summit Eye contracted with Eye Care Leaders to provide myCare Integrity, an Electronic Medical Records solution.

100. On or about April 27, 2022, Ms. Sandvig received a mailed Notice of Data Breach Letter, related to Eye Care Leaders' December 2021 Data Breach. *See* Plaintiff's Notice Letter, attached as Exhibit A.

101. The Notice Letter that Plaintiff received listed an extensive amount of her PII and PHI was in files that were "removed" from Eye Care Leaders' network. It stated that her full name was among the files that "may have been accessed or acquired" along with one or more of the following: Social Security number, information regarding care received at Summit Eye, date of birth, medical record number, and/or health insurance information." *See* Plaintiff's Notice Letter, attached as Exhibit A.

102. Ms. Sandvig is alarmed by the amount of her Private Information that was stolen or accessed as listed on her letter, and even more by the fact that her Social Security number was identified as among the breached data on Eye Care Leaders' computer system.

103. Since Eye Care Leaders' Data Breach, Ms. Sandvig was the victim of Identity Theft. Ms. Sandvig's email was hacked into. She discovered that someone had accessed her email and changed her email address from "cs.com" to "compuserve.com."

104. Since the Data Breach, Ms. Sandvig has been receiving a significantly higher number of spam emails and texts.

105. Since the Eye Care Leaders Data Breach, Ms. Sandvig monitors her accounts monthly. In particular, Ms. Sandvig goes through her Discover, American Express, Savings, and Checking accounts to ensure she recognizes each charge. She now spends about approximately 15-30 minutes inspecting her accounts for unidentified charges, much more than he spent monitoring her accounts in the past.

106. Furthermore, since the Eye Care Leader Data Breach. Ms. Sandvig has been required to take time out of her day to discuss the Data Breach over the phone with Compuserve and McAfee, a virus protection company.

107. Upon information and belief, these telephone discussion last approximately an hour and a half to two hours per discussion.

108. As a result of Eye Care Leaders' Data Breach, Ms. Sandvig has experienced increased anxiety.

109. Ms. Sandvig is aware that cybercriminals often sell Private Information, and that hers could be abused months or even years after a data breach.

110. Had Ms. Sandvig been aware that Eye Care Leaders' computer systems were not secure, she would not have entrusted Eye Care Leaders with her Private Information.

Plaintiff's and Class Members' Damages

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

112. Moreover, Eye Care Leaders has offered only a paltry one year of identity theft monitoring and identity theft protection through IDX. This one-year limitation is inadequate when victims are likely to face many years of identity theft.

113. Eye Care Leaders' credit monitoring offer and advice to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In other words, Eye Care Leaders expects Plaintiff and Class to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

114. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII and PHI.

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

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

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

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

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

120. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Part of the price Summit Eye, on behalf of Class members, paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and Plaintiff's and Class Members' Private Information. Thus, Summit Eye, Plaintiff and the Class Members did not get what they paid for. Specifically, they overpaid for services that were intended to be accompanied by adequate data security but were not.

121. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

122. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

123. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach.

124. In addition, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

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

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

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

CLASS ACTION ALLIGATIONS

126. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated (the "Class") pursuant to Federal Rule of Civil Procedure 23.

127. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was compromised as a result of the Data Breach discovered by Defendant Eye Care Leaders on or about December 4, 2021 (the "Class"), including all persons who were sent a notice of the Data Breach.

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

129. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

130. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately 342,000 consumers whose data was compromised in the Data Breach.

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

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

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

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

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

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

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

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

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

i. Whether Defendant's conduct was negligent, and;

j. Whether Plaintiff and Class Members are entitled to damages and/or injunctive relief.

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

133. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

134. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

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

136. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

137. 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 failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant's failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

138. Finally, all members of the proposed Class are readily ascertainable.Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSE OF ACTION
Count I
Negligence
(On Behalf of Plaintiff and All Class Members)

139. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

140. Summit Eye required Plaintiff and Class Members to submit non-public personal information in order to obtain medical services.

141. Summit Eye then submitted non-public personal information to Defendant.

142. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach

143. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

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

145. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

146. Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

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

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

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

b. Failing to adequately monitor the security of its networks and systems;

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

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

e. Failing to abide by its website promise of complying with all federal healthcare laws;

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

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

h. Failing to have mitigation and back-up plans in place in the event of a Data Breach and data breach.

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

151. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

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

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

Count II
Invasion of Privacy
(On Behalf of Plaintiff and All Class Members)

154. Plaintiff repeats and incorporates by reference each allegation in the above paragraphs as if fully set forth herein.

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

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

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

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

159. Defendant intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

160. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

161. Plaintiff sustained damages (as outlined above) as a direct and proximate consequence of the invasion of her privacy by intrusion, and therefore seeks an award of damages on behalf of herself and the Class.

Count III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and All Class Members)

162. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

163. In providing their Private Information to Defendant, Plaintiff and Class Members justifiably placed special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and Class Members to safeguard and keep confidential that Private Information.

164. Defendant Eye Care Leaders accepted the special confidence placed in it by Plaintiff and Class Members.

165. Additionally, although Defendant acknowledges on its website to comply with federal healthcare laws, including the duty to protect Private Information, it failed to do so.

166. There was an understanding between Plaintiff and the Class Members and Summit Eye that Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of the Private Information.

167. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members, for the safeguarding of Plaintiff's and Class Members' Private Information.

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

169. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach and data breach in a reasonable and practicable period of time.

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

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

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

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

174. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

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

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

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

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

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

180. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

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

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

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

184. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

185. WHEREFORE, Plaintiff prays for judgment as follows:

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

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

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

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

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

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

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this Complaint so triable. Plaintiff also respectfully requests leave to amend this Complaint to conform to the evidence, if such amendment is needed for trial.

Dated: June 10, 2022

Respectfully Submitted,

By: /s/ Joel R. Rhine

Joel R. Rhine
NCSB # 16028
Rhine Law Firm, P.C.
1612 Military Cutoff Road
Suite 300
Wilmington, NC 28403
Tel: (910) 772-9960
JRR@rhinelawfirm.com

Gary E. Mason
gmason@masonllp.com
Danielle L. Perry*
dperry@masonllp.com
Lisa A. White
lwhite@masonllp.com
MASON LLP
5101 Wisconsin Ave. NW Ste. 305
Washington DC 20016
Phone: 202.640.1160
Fax: 202.429.2294

Ben Barnow*
b.barnow@barnowlaw.com
Anthony L. Parkhill*
aparkhill@barnowlaw.com
Riley W. Prince*
rprince@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Telephone: (312) 621-2000
Facsimile: (312)641-5504

Attorneys for Plaintiff and the Class

**pro hac vice forthcoming*