UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IAN TORRES, on behalf of himself and all others similarly situated, Plaintiff, v. **U.S. VISION, INC.** and **USV OPTICAL, INC.** Defendants.	Case No. Judge **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Ian Torres ("Plaintiff") brings this Class Action Complaint, on behalf of himself and all others similarly situated (the "Class Members"), against Defendants U.S. Vision, Inc. ("U.S. Vision") and USV Optical, Inc. ("USV Optical") (collectively "Defendants") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

NATURE OF CASE

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") on U.S. Vision's network that resulted in unauthorized access to highly sensitive patient data.[1] As a result of the Data Breach, Plaintiff and approximately 180,000 other Class Members[2] suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses, and

[1] https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-658.pdf
[2] https://www.hipaajournal.com/u-s-vision-subsidiary-reports-hacking-incident-affecting-180000-individuals/ (last accessed 10/09/2022)

the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information.

2. The specific information compromised in the Data Breach includes personally identifiable information ("PII"), such as full names, addresses, dates of birth, Social Security numbers, taxpayer identification numbers, driver's license numbers, and financial account information, as well as protected health information ("PHI"), such as medical treatment and diagnosis information, medical record numbers, dates of service, provider names, diagnosis and symptom information, prescription/medication information, health insurance information (including payor and subscriber Medicare/Medicaid numbers), and billing and claims information (collectively, PII and PHI are "Private Information").

3. Upon information and belief, prior to and through May 27, 2021, Defendants obtained the Private Information of Plaintiff and Class Members and stored that Private Information, unencrypted, in an Internet-accessible environment on Defendants' network.

4. Plaintiff and Class Members' Private Information—which was entrusted to Defendants, their officials, and agents—was compromised and unlawfully accessed due to the Data Breach.

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of his and Class Members' Private Information that Defendants collected and maintained, and for Defendants' failure to provide timely and adequate notice to Plaintiff and other Class Members that their Private Information had been subject to the unauthorized access of an unknown third party.

6. Defendants maintained the Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on Defendants' computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. In addition, upon information and belief, Defendants and their employees failed to properly monitor the computer network and IT systems that housed Plaintiff's and Class Members' Private Information.

8. Plaintiff and Class Members' identities are now at risk because of Defendants' negligent conduct because the Private Information that Defendants collected and maintained is now in the hands of malicious cybercriminals.

9. Defendants failed to provide timely, accurate and adequate notice to Plaintiff and Class Members. Plaintiff and Class Members' knowledge about the Private Information Defendants lost, as well as precisely what type of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Defendants' failure to warn impacted persons for approximately seventeen (17) months after first learning of the data breach.

10. In letters dated October 28, 2022, multiple eye care companies, including Nationwide Vision Center, LLC, Nationwide Optometry, P.C. and SightCare, Inc., by and though Nationwide Optical Group, LLC, notified state Attorneys General and many Class Members about

the widespread data breach that had occurred on Defendants' computer network and that Class Members' Private Information was accessed and acquired by malicious actors.[3]

11. In its required Notice Letter Nationwide Optical, LLC explained that it had acquired or became affiliated with several entities from U.S. Vision in September 2019 and that it had a continuing business relationship with Defendant, stating that Defendant U.S. Vision provided "some administrative services as a business associate to us."[4]

12. The Notice Letter stated that on May 12, 2021 (17 months earlier) Defendants "became aware of suspicious activity involving its computer network."[5] Defendants then notified Nationwide Optical Group, LLC of this suspicious activity on May 12, 2021, but did not identify or notify the individual entities or patients who had their data stolen. Defendants did not disclose the identities of the individual entities whose data was accessed and to Nationwide Optical Group, LLC until September 22. 2022.[6] After learning the identities of the affected persons and entities, Nationwide Optical Group, LLC still took over a month to notify state Attorneys General and Class Members about the widespread Data Breach.

13. Defendants posted a notice of the Data Breach their website (the "Website Notice") acknowledging their investigation into the Data Breach determined that "records related to certain customers and employees may have been viewed and/or taken by an unauthorized individual as a result of this incident." The Website Notice further admitted that the Private Information included "individuals name, eyecare insurance information including policy and/or subscription information,

[3] https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-658.pdf (last accessed November 9, 2022) (the "Notice Letter")
[4] *Id.*
[5] *Id.*
[6] *Id.*

eyecare insurance application and/or claims information, and for a smaller number of individuals may include address, date of birth, and/or other individual identifiers."[7]

14. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including 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.

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

16. Plaintiff and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

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

18. Accordingly, Plaintiff brings claims on behalf of himself and the Class for: (i) negligence, (ii) breach of implied contract; and (iii) unjust enrichment. Through these claims,

[7] https://www.usvision.com/wp-content/uploads/2021/09/USV-Website-Notice.pdf (last accessed November 9, 2022).

Plaintiff seeks, *inter alia*, damages and injunctive relief, including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services.

THE PARTIES

19. Plaintiff Ian Torres is a natural person, resident, and a citizen of the State of Arizona. Plaintiff Torres has no intention of moving to a different state in the immediate future. Plaintiff Torres is acting on his own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff Torres' Private Information and owed him a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Torres would not have entrusted his Private Information to Defendants, their officials, and agents, had he known that Defendants failed to maintain adequate data security. Plaintiff Torres' Private Information was compromised and disclosed as a result of Defendants' inadequate data security, which resulted in the Data Breach.

20. Plaintiff received a notice letter from Nationwide Vision and SightCare, Inc. dated October 28, 2022, stating that a data security incident occurred at USV Optical, Inc., a subsidiary of U.S. Vision, Inc. and that his personal information was involved in the incident.

21. Defendant U.S. Vision, Inc., a wholly-owned subsidiary of Refac Optical, Inc, is a retail optical chain that provides eye care services and administration for healthcare providers around the country and has over 350 locations nationwide.[8] U.S. Vision is incorporated in the State of Delaware and its principal place of business is located at 1 Harmon Drive, Blackwood, New Jersey 08012.

[8] https://www.usvision.com/about-us/(last accessed November 8, 2022).

22. Defendants USV Optical, Inc., is a wholly owned subsidiary of U.S. Vision, Inc. Defendant USV Optical, Inc.'s principal place of business is also located at 1 Harmon Drive, Blackwood, New Jersey 08012.

JURISDICTION AND VENUE

23. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the putative Class, as defined below, are citizens of a different state than Defendants, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

24. This Court has general personal jurisdiction over Defendants because Defendants maintain principal places of business at 1 Harmon Drive, Glendora, New Jersey 08029 regularly conducts business in New Jersey, and has sufficient minimum contacts in New Jersey. Defendants intentionally availed itself of this jurisdiction by marketing and selling its services from New Jersey to many businesses nationwide.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants' principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

DEFENDANTS' BUSINESSES

26. U.S. Vision, Inc. provides eye care services and administration for healthcare providers around the country and has over 350 locations nationwide.[9] Defendants claim, "We take this incident and the security of information in our care seriously."[10]

[9] https://www.usvision.com/about-us/(last accessed November 8, 2022).
[10] https://www.usvision.com/wp-content/uploads/2021/09/USV-Website-Notice.pdf.pdf (last accessed November 8, 2022).

27. U.S. Vision, Inc. is a national provider of managed vision care benefits.[11]

28. USV Optical, Inc. is a subsidiary of U.S. Vision, Inc. and is a retailer of optical products and services.

29. Upon information and belief, U.S. Vision, Inc. and USV Optical, Inc. maintain and share the same computer network.

30. On information and belief, in the ordinary course of medical practice management and administrative services, Defendants maintain the Private Information of patients and customers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Medication information,
- Health insurance information,
- Photo identification;
- Employment information, and;
- Other information that Defendants may deem necessary to provide care.

[11] https://www.linkedin.com/company/us-vision/about/ (last accessed November 8, 2022).

31. Additionally, Defendants may receive Private Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), close friends, and/or family Members.

32. On information and belief, Defendants provided medical practice management and administrative services for Nationwide Vision where Plaintiff was a patient.

33. Because of the highly sensitive and personal nature of the information Defendants acquire and store with respect to patients, Defendants, upon information and belief, promise to, among other things: keep Private Information private; comply with healthcare industry standards related to data security and Private Information; inform customers and patients of its legal duties and comply with all federal and state laws protecting customers' and patients' Private Information; only use and release customers' Private Information for reasons that relate to medical care and treatment; and provide adequate notice to customers if their Private Information is disclosed without authorization.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

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

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

THE CYBERATTACK

37. On or around, May 12, 2021, Defendants became aware of suspicious activity in its network environment.

38. Defendants investigated the suspicious activity with the assistance of a third-party computer forensic specialist.

39. Through investigation, Defendants determined that its network and servers were subject to a cyber-attack that impacted its network where information on its network was accessed and acquired without authorization.

40. The investigation determined that files related to certain customers and employees on Defendants' network were accessed and taken by an unauthorized user between April 20, 2021 and May 17, 2021.

41. Upon information and belief, Plaintiff's and Class Members' Private Information was exfiltrated and stolen in the attack.

42. Upon information and belief, the accessed systems contained Private Information and that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

43. It is likely the Data Breach was targeted at Defendants due to their status as healthcare providers that collect, create, and maintain both PII and PHI.

44. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the Private Information of Plaintiff and the Class Members.

45. Defendants admitted that the stolen information may have included full names, addresses, dates of birth, Social Security Numbers, taxpayer identification numbers, driver's license

numbers, financial account information, medical treatment and diagnosis information, including medical record numbers, dates of service, provider names, diagnosis and symptom information, prescription/mediation information, and health insurance information including payor and subscriber Medicare/Medicaid numbers, and billing and claims information.

46. While Defendants stated in the notice letter that the unusual activity occurred and was discovered in April 2021, Defendants did identify the specific persons or entities whose Personal Information was acquired and exfiltrated until October 2022– approximately 17 months later.

47. Upon information and belief, and based on the type of cyberattack, it is plausible and likely that Plaintiff's Private Information was stolen in the Data Breach. Plaintiff further believes his Private Information was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of all cybercriminals.

48. As Defendants acknowledge in their Notice Letters, Defendants take "the security of information in our care seriously."[12]

49. Defendants had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' Private Information from involuntary disclosure to third parties.

50. In response to the Data Breach, Defendants admit they worked with "computer forensic specialists" to "determine the nature and scope of the incident" and purports to have "took steps to secure our systems." Defendants admit additional security was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' Private Information going forward.

[12] See Notice Letter, https://www.usvision.com/wp-content/uploads/2021/09/USV-Website-Notice.pdf (last accessed November 8, 2022).

51. Because of the Data Breach, data thieves were able to gain access to Defendants' IT systems for 27 days (between April 20, 2021, and May 17, 2021) and were able to compromise, access, and acquire the protected Private Information of Plaintiff and Class Members.

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

53. Plaintiff and the Class Members reasonably relied (directly or indirectly) on this sophisticated eye care institution to keep their sensitive Private Information confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their Private Information.

54. Plaintiff's and Class Members' unencrypted, unredacted Private Information was compromised due to Defendants negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' Private Information. Criminal hackers obtained their Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The risks to Plaintiff and Class Members will remain for their respective lifetimes.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

55. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

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

57. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[13] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[14] The 330 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.[15]

58. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendants knew or should have known that its electronic records would be targeted by cybercriminals.

59. Indeed, cyberattacks on medical systems like Defendants have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[16]

---

[13] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[14] *Id.*
[15] *Id.*
[16] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited June 23, 2021).

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

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

Defendants Fail to Comply with FTC Guidelines

62. 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.

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

---

[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.

[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 visited Jan. 19, 2022).

[19] *Id*.

64. 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.

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

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

67. Defendants failed to properly implement basic data security practices.

68. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

69. Defendants were at all times fully aware of its obligation to protect the Private Information of customers and patients. Defendants were also aware of the significant repercussions that would result from its failure to do so.

Defendants Fail to Comply with Industry Standards

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

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

72. 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.

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

74. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Defendants' Conduct Violates HIPAA and Evidences Their Insufficient Data Security

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

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

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

78. A Data Breach such as the one Defendants 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

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

DEFENDANTS' BREACH

80. Defendants breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard their computer

systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

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

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

e. Failing to train their employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

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

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

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

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

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

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

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

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

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

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and,

q. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' Private Information.

81. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access Defendants' computer network and systems which contained unsecured and unencrypted Private Information.

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

Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft

83. Cyberattacks and data breaches at healthcare companies like Defendants are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

84. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[20]

85. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[21]

[20] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

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

86. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[22]

87. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

88. 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

[22] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

identity), 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.[23]

89. 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.

90. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

91. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[24]

92. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

93. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider,

---

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

[24] *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).

or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[25]

94. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information 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.

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

96. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

97. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

98. 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.

---

[25] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Jan. 19, 2022).
[26] GAO Report, at p. 29.

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

100. Private Information can sell for as much as $363 per record according to the Infosec Institute.[27] 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.

101. 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.[28] 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.[29] Each of these fraudulent activities is difficult to detect. An individual may not know that his or his 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.

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

103. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old

[27] *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/.
[28] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (Jan. 19, 2022).
[29] *Id* at 4.

number, so all of that old bad information is quickly inherited into the new Social Security number."[30]

104. 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."[31]

105. Medical information is especially valuable to identity thieves.

106. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[32] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[33]

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

108. For this reason, Defendants knew or should have known about these dangers and strengthened their data and email handling systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendants failed to properly prepare for that risk.

---

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

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

[32] *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/.

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

Plaintiff's and Class Members' Damages

109. To date, Defendants have done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

110. Defendants have merely offered Plaintiff and Class Members complimentary fraud and identity monitoring services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

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

112. Plaintiff and Class Members' full names, addresses, dates of birth, Social Security Numbers, taxpayer identification numbers, driver's license numbers, financial account information, medical treatment and diagnosis information, including medical record numbers, dates of service, provider names, diagnosis and symptom information, prescription/mediation information, and health insurance information including payor and subscriber Medicare/Medicaid numbers, and billing and claims information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendants' computer network.

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

114. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring his accounts for fraudulent activity.

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

116. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff was recently alerted by the Internal Revenue Service that an unauthorized third party attempted to file a fraudulent tax return under his name.

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

118. 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.

119. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members. Plaintiff has already experienced various phishing attempts by telephone and through electronic mail.

120. 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.

121. 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.

122. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendants was intended to be used by Defendants to fund adequate security of Defendants' computer system and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for and agreed to.

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

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

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

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

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

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

Plaintiff Torres' Experience

128. Plaintiff Torres received eye care from Nationwide Vision when he was a minor. Nationwide Vision, LLC, Nationwide Optometry, and SightCare, Inc. then subsequently affiliated with or were acquired by Nationwide Optical Group, LLC. Nationwide Optical Group, LLC was a business associate of Defendants and utilized Defendants for eye care management and administrative services.

129. Upon information and belief, Plaintiff Torres was presented with standard medical forms to complete prior to his service that requested his PII and PHI, including HIPAA and privacy disclosure forms.

130. As part of his care and treatment, and as a requirement of services, Plaintiff Torres entrusted his Private Information to his medical providers and their agents or affiliates with the reasonable expectation and understanding that they would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify his of any data security incidents related to his. Plaintiff Torres would not have provided his Private Information or used these services had he known that Defendants would not take reasonable steps to safeguard his Private Information.

131. Plaintiff Torres first learned of the Data Breach after receiving a data breach notification letter dated October 28,2022 from Nationwide Optical Group, LLC, notifying him that Defendants suffered a data breach 17 months prior and that his Private Information had been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendants.

132. The data breach notification letter indicated that the Private Information involved in the Data Breach may have included Plaintiff Torres's full name, address, date of birth, Social Security Number, taxpayer identification number, driver's license number, financial account information, medical treatment and diagnosis information (including medical record numbers, dates of service, provider names, diagnosis and symptom information), prescription/medication information, and health insurance information including payor and subscriber Medicare/Medicaid numbers, and billing and claims information.

133. As a result of the Data Breach, Plaintiff Torres made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

134. Plaintiff Torres experienced actual identify theft and fraud, which he discovered after receiving a letter from the U.S. Internal Revenue Service (the "IRS Letter"), dated September 29, 2022, explaining that an unauthorized person attempted to impersonate Plaintiff Torres by using his name and taxpayer ID number to file a false tax return. The IRS Letter stated that Plaintiff Torres may be the victim of identity theft.

135. As a result of the attempted fraud on Plaintiff Torres' tax return, the IRS placed an identity theft indicator on Plaintiff Torres' taxpayer identification number that will be reviewed by the IRS on all future tax returns filed by Plaintiff Torres. Plaintiff Torres must also use a identify protection personal ID number ("IP PIN") that he must use on all future tax returns for the remainder of his life. This unique ID PIN changes each December or January. As a result, Plaintiff Torres must continually acquire and enter a new ID PIN for every tax return he files for the remainder of his life.

136. The IRS Letter further suggested that Plaintiff Torres monitor his financial accounts for suspicious or unusual activity and directed to contact certain identify theft partners provided by the IRS if suspicious activity occurred.

137. Plaintiff Torres has spent multiple hours and will continue to spend valuable time for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

138. Plaintiff Torres suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendants obtained from Plaintiff Torres; (b) violation of his privacy rights; (c) the theft of his Private Information; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

139. As a result of the Data Breach, Plaintiff Torres has also suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Torres is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff also has suffered anxiety about unauthorized parties viewing, using, and/or publishing of information related to his medical records and prescriptions.

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

CLASS ACTION ALLEGATIONS

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

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

> **All persons identified by Defendants (or their agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").**

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

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

145. 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 at least 180,000[34] individuals whose sensitive data was compromised in the Data Breach.

146. 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 Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendants 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 Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

[34] https://www.hipaajournal.com/u-s-vision-subsidiary-reports-hacking-incident-affecting-180000-individuals/ (last accessed 10/09/2022).

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

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

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

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

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

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

j. Whether Defendants' conduct was negligent;

k. Whether Defendants breach implied contracts with Plaintiff and Class Members;

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

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

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

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

148. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

149. Predominance. Defendants have 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 system and unlawfully accessed in the same way. The common issues arising from Defendants' 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.

150. 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 Defendants. 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.

151. Defendants 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.

152. Likewise, particular issues under Rule 42(d)(l) 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 Defendants failed to timely notify the public of the Data Breach;

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

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

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

e. Whether Defendants 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.

153. Finally, all members of the proposed Class are readily ascertainable. Defendants 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 Defendants.

CAUSES OF ACTION

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

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

155. Defendants required individuals through their eye care provider partners, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of healthcare services.

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

157. Defendants 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 their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

158. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a

superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

159. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

160. In addition, Defendants 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.

161. Defendants' 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 Defendants are bound by industry standards to protect confidential Private Information.

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

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

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

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

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

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

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

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

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

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

165. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendants had a duty to implement reasonable safeguards to protect Plaintiff and Class Members' Private Information.

166. Pursuant to HIPAA, Defendants had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, 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." *See* definition of encryption at 45 C.F.R. § 164.304.

167. Defendants breached their duties to Plaintiff and Class Members under HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

168. Defendants owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiff's and Class Members' Private Information.

169. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendants hold vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the Private Information—whether by malware or otherwise.

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

171. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiff and Class Members—which actually and proximately caused the Data Breach and injured Plaintiff and Class Members.

172. Defendants further breached their duties by failing to provide reasonably timely notice of the data breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiff and Class Members' injuries-in-fact.

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

173. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

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

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

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

176. Plaintiff and the Class were required to and delivered their Private Information to Defendants or Defendants' partners or business associates as part of the process of obtaining services provided by Defendants. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendants in exchange for services.

177. Defendants, and their partners or business associates solicited, offered, and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

178. Defendants accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

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

180. In delivering their Private Information to Defendants and providing paying for healthcare services, Plaintiff and Class Members intended and understood that Defendants would adequately safeguard the data as part of that service.

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

182. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6)

multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

183. Plaintiff and the Class Members would not have entrusted their Private Information to Defendants in the absence of such an implied contract.

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

185. Defendants recognized that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

186. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendants.

187. Defendants breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

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

THIRD COUNT
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

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

190. This count is pleaded in the alternative to breach of implied contract.

191. Upon information and belief, Defendants funds their data security measures entirely from their general revenue, including payments made by or on behalf of Plaintiff and the Class Members and from partner eye care providers.

192. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

193. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and/or their agents and in so doing provided Defendants with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

194. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

195. Plaintiff and Class Members conferred a monetary benefit on Defendants, by paying Defendants as part of Defendants rendering of eye care related services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' Personal Information, and by providing Defendants with their valuable Personal Information.

196. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members,

on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

197. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

198. Defendants acquired the monetary benefit and Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

199. If Plaintiff and Class Members knew that Defendants had not secured their Personal Information, they would not have agreed to provide their Personal Information to Defendants.

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

201. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Personal Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Personal Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Personal Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest,

and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

202. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

203. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and his counsel as Class Counsel;

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

c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

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

e) Ordering Defendants to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: November 10, 2022

Respectfully Submitted,

/s/ *Victoria Maniatis*
Victoria Maniatis
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: (212) 594-5300
vmaniatis@milberg.com

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

Attorneys for Plaintiff and the Proposed Class

** Pro Have Vice Forthcoming*