UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

HEATHER BOWEN and BENJAMIN F. LIANG on behalf of themselves and all others similarly situated, **Plaintiffs,** **v.** **20/20 EYE CARE NETWORK, INC., and ICARE HEALTH SOLUTIONS, LLC,** **Defendants.**	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Heather Bowen and Benjamin J. Liang ("Plaintiffs"), by and through their attorneys, upon personal knowledge as to themselves and their own acts and experiences, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this Class Action Complaint ("Complaint") against Defendants 20/20 Eye Care Network, Inc. ("Eye Care") and iCare Health Solutions, LLC ("iCare") (collectively "Defendants"), individually and on behalf of all others similarly situated, based on Defendants' failure to properly safeguard current and former patients' personally identifiable information ("PII"), including patients' names, dates of birth, social security numbers, and protected health information ("PHI"), including patients' member identification numbers and health insurance information.

2. Eye Care is a large corporation that acts as a third-party plan administrator with respect to hearing and vision insurance, and assists insurance companies and patients with claims processing, credentialing of professionals, and linking patients with in-network providers.

3. Upon information and belief, iCare is an integrated specialty network and administrator backed by private equity firm Pine Tree Equity IV, LP, that invested in Eye Care and, in whole or in part, controls Eye Care in connection with its administration and management of over 55 ophthalmology and optometry locations across the state of Florida.

4. On January 11, 2021, Eye Care was alerted to suspicious activity in its Amazon Web Services ("AWS") environment. Over a month later, it confirmed that as a result of "insider wrongdoing," S3 buckets hosted in AWS had been accessed, data in those buckets had been downloaded, and then all data in the S3 buckets was deleted (the "Data Breach").[1]

5. In total, the Data Breach may have compromised the PII and PHI of more than 3.2 million individuals ("Class Members").

6. Shockingly, Eye Care did not begin notifying the individual victims of the Data Breach until May of 2021. For example, Plaintiffs were first notified about the Data Breach in a letter dated May 28, 2021.

7. Eye Care did not adequately safeguard Plaintiffs' data, and now they, and millions of other individuals, are the victims of a significant Data Breach that puts them at a significantly increased risk of identity fraud and negatively will impact them for years.

8. Eye Care is responsible for allowing this Data Breach through its failure to implement and maintain reasonable data security safeguards, failure to exercise reasonable care in the hiring and supervision of its employees and agents, and failure to comply with industry-

[1] "Amazon S3 is an object store that uses unique key-values to store as many objects as you want. You store these objects in one or more buckets, and each object can be up to 5 TB in size." Amazon S3 objects overview, AWS, https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingObjects.html (last visited June 21, 2021). "Objects consist of the file data and metadata that describes the object. You can have an unlimited number of objects in a bucket." Uploading objects, AWS, https://docs.aws.amazon.com/AmazonS3/latest/userguide/upload-objects.html (last visited June 21, 2021).

standard data security practices as well as federal and state laws and regulations governing data security and privacy, including security of PII and PHI.

9. Despite their role in managing so much sensitive and personal PII and PHI, Defendants failed to recognize and detect unauthorized third parties accessing its system, and failed to recognize the substantial amounts of data that had been compromised.

10. Defendants failed to, among other things, detect that ill-intentioned criminals had accessed their computer data and storage systems, notice the massive amounts of data that was compromised, and take any steps to investigate the red flags that should have warned Defendants that their systems were not secure. Had Defendants properly maintained and monitored their information technology infrastructure, they would have discovered the invasion sooner – and/or prevented it altogether.

11. Defendants had numerous statutory, regulatory, and common law duties to Plaintiffs and Class Members to keep their PII, including PHI, confidential, safe, secure, and protected from unauthorized disclosure or access, including duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Plaintiffs and Class Members rely upon Defendants to maintain the security and privacy of the PII entrusted to them; when providing their PII to Defendants' clients, they reasonably expected and understood that Defendants would ensure that they, their vendors, and their clients would comply with the obligation to keep Plaintiffs' PII secure and safe from unauthorized access.

12. In this era of frequent data security attacks and data breaches, particularly in the healthcare industry, Defendants' failures leading to the Data Breach are particularly egregious.

13. By obtaining, collecting, using, and deriving benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

14. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI.

15. Plaintiffs and Class Members relied on Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

16. As a result of Defendants' failures to protect the PII and PHI of Plaintiffs and Class Members, their PII and PHI were accessed and downloaded by malicious cyber criminals, who targeted that information through their "wrongdoing." As a direct and proximate result, Plaintiffs and Class Members are now at a significant present and future risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come. Common sense dictates that this was the sole reason the unauthorized actors breached Defendants' system and acquired Plaintiffs' and Class Members' sensitive PII and PHI.

17. Plaintiffs and Class Members have now lost the economic value of their PII and PHI. Indeed, there is both a healthy black market and a legitimate market for that PII and PHI. Just as Plaintiffs' and Class Members' PII and PHI were stolen, *inter alia*, because of its inherent value in the black market, the inherent value of Plaintiffs' and Class Members' PII and PHI in the legitimate market is now significantly and materially decreased. To make matters worse, Plaintiffs' and Class Members' injuries described herein were exacerbated by Defendants' failure to timely inform and notify Plaintiffs and Class Members of the Data Breach and the theft of their PII and PHI. Furthermore, by failing to provide adequate notice, Defendants prevented Plaintiffs

and prospective Class Members from taking actions to protect themselves and attempt to mitigate the harm.

18. Plaintiffs and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their PII and PHI; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (e) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (f) damages to and diminution in value of their personal data entrusted to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' PII and PHI against theft and not allow access and misuse of their personal data by others; (g) the reasonable value of the PII and PHI entrusted to Defendants; and (h) the continued risk to their PII and PHI, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII and PHI.

19. Plaintiffs seek to remedy these harms, and to prevent their future occurrence, on behalf of themselves and all similarly situated persons whose PII and PHI were compromised as a result of the Data Breach.

20. Accordingly, Plaintiffs, on behalf of themselves and other Class Members, assert claims for negligence, negligence *per se*, and declaratory judgment. Plaintiffs also assert claims on behalf two subclasses: a subclass of Florida residents under the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §501.201, *et seq.* ("FDUTPA") and, a subclass of Pennsylvania

residents under the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§202-1, *et seq.* Plaintiffs seek injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Plaintiff Heather Bowen

21. Plaintiff Bowen is a natural person and a resident of Pennsylvania.

22. Plaintiff Bowen received a letter dated May 28, 2021 from Eye Care concerning the Data Breach. The letter stated her name, Social Security number, member identification number, date of birth, and health insurance information may have been compromised in the Data Breach.

23. Plaintiff Bowen has sought treatment for several eye and ear problems and has seen several medical providers related to those issues over the years in both Florida, where she lived for roughly four years between 2013 and 2018, and Pennsylvania, where she lives now and has for most of her life. She provided those providers with her PII and PHI in order to receive treatment services.

24. The letter provided Plaintiff Bowen a number to call for more information about the Data Breach. Plaintiff called this number and requested information about the Data Breach.

25. As a result of the Data Breach, Plaintiff Bowen faces a substantial risk of imminent identity, financial, and health fraud and theft—both now and for the rest of her life.

26. Since learning about the Data Breach, Plaintiff Bowen has suffered and continues to suffer emotional anguish and distress, including but not limited to fear, anxiety, and stress related to the compromise and theft of her PII and PHI.

27. Furthermore, Plaintiff Bowen has spent increased time reviewing her financial statements to determine whether there has been any fraudulent activity on her accounts. For

example, as a result of the Data Breach, she now checks her bank statement multiple times a day. She will continue to spend additional time every month to review her statements due to the increased risk of identity theft posed by the unlawful disclosure of her PII and PHI.

28. Plaintiff Bowen has also spent several hours changing various account passwords, speaking on the phone about the Data Breach with entities such as her insurance providers, and researching the Data Breach. She also plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach, such as replacing her debit card, placing fraud alerts on her credit through the credit bureaus, and upon the advice of her insurance provider, obtaining a new Medicare number.

Plaintiff Benjamin Liang

29. Plaintiff Liang is a natural person and a resident of Florida.

30. Plaintiff Liang received a letter dated May 28, 2021 from Eye Care concerning the Data Breach. The letter stated his name, date of birth, Social Security number, member identification number, and health insurance information may have been viewed, seen, or accessed in the Data Breach.

31. Plaintiff Liang has sought treatment for eye issues and has seen medical providers related to those issues over the years in Florida. He provided those providers with his PII and PHI in order to receive treatment services.

32. As a result of the Data Breach, Plaintiff Liang faces a substantial risk of imminent identity, financial, and health fraud and theft—both now and for the rest of his life.

33. Since learning about the Data Breach, Plaintiff Liang has suffered and continues to suffer emotional anguish and distress, including but not limited to fear, anxiety, and stress related to the compromise and theft of his PII and PHI. He is worried about the Data Breach's impact on

his PII and PHI and is fearful that he will be required to continue zealously monitoring his identity, credit, and other PII and PHI for perhaps the rest of his life.

34. Plaintiff Liang has spent increased time reviewing his financial statements and credit, including on Credit Karma and through his American Express account, to determine whether there has been any fraudulent activity on his accounts. For example, as a result of the Data Breach, he now checks his bank accounts and credit multiple times daily. He will continue to spend additional time every week to review his statements and credit due to the increased risk of identity theft posed by the unlawful disclosure of his PII and PHI.

35. Furthermore, Plaintiff Liang has experienced an increased amount of robocalls since the Data Breach.

36. The Data Breach notices Plaintiffs received offered them a one-year membership to a single bureau credit monitoring from credit reporting agency, TransUnion. This service only monitors fraudulent activity reported to Transunion. Fraudulent activity reported to other reporting bureaus, such as Equifax and Experian, would not be monitored under the proffered service.

37. The Data Breach notices further state: "We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." The letter advised Plaintiffs they had the right to obtain "one free credit report annually from each of the three major credit reporting bureaus." Despite urging Plaintiffs to "check [their] credit reports," Defendants did not offer to pay costs associated with Plaintiffs obtaining more than "one free credit report annually…."

38. The Data Breach notices also advised Plaintiffs of their right to obtain a security freeze on his credit report. However, it acknowledged that "using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay,

interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit."

Defendant Eye Care and Hearing Care

39. Defendant 20/20 Eye Care Network, Inc. is a Florida corporation with its principal place of business in Ft. Lauderdale, Florida. It also does business under the registered fictitious name, 20/20 Hearing Care Network, Inc. ("Hearing Care").

40. Eye Care contracts with optometrists, ophthalmologists, and eye care facilities to link them with plan participants. Eye Care acts as a third-party plan administrator, assisting insurance companies and patients with claims processing, credentialing of professionals, and linking patients with an in-network providers.

41. Hearing Care similarly manages a network of audiologists to refer managed care members to, acting as a middle-man between managed care plans and their members. It manages patient benefits by answering patient inquiries and grievances, recruiting healthcare providers to the network, reviewing professional credentials, and processing medical claims/prescriptions. It also contracts to provide hearing aid products.

Defendant iCare

42. Defendant iCare Health Solutions, LLC is a Florida limited liability company with its principal place of business in Miami, Florida.

43. In September 2020, iCare invested in Eye Care, and controls Eye Care in providing vision care in conjunction with over 55 owned locations across the state of Florida.

JURISDICTION & VENUE

44. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2), because this is a putative class action involving more than 100 Class Members and

because the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Moreover, Plaintiff Bowen and Defendants are citizens of different states.

45. This Court has general personal jurisdiction over Defendants Eye Care and iCare because Defendants are Florida entities and have their principal places of business in Ft. Lauderdale, Florida, and Miami, Florida, respectively.

46. Venue is proper in this District under 28 U.S.C. §§1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendants conduct substantial business in this District.

FACTUAL ALLEGATIONS

The Data Breach

47. On January 11, 2021, Eye Care was alerted to suspicious activity in its Amazon AWS environment. It later discovered that S3 buckets hosted in AWS had been accessed, data in those buckets had been downloaded, and then all data in the S3 buckets was deleted.

48. In late February 2021, Eye Care determined the data potentially included the PII and PHI of more than 3.2 million health plan members for whom it held records.

49. Eye Care provided notice to the Maine Attorney General ("Maine AG") that described the Data Breach as "insider wrongdoing."[2] This description indicates that Eye Care's

[2] Data Breach Notifications, Maine Atty. Gen., https://apps.web.maine.gov/online/aeviewer/ME/40/946029d6-7945-4a23-89c1-0ea29e9c18a2.shtml (last visited June 21, 2021). The Maine AG requires that businesses suffering a data breach involving residents of Maine must submit notice to the Maine AG on a form provided by the Maine AG's office. See Maine Security Breach Reporting Form, Maine Atty. Gen., https://appengine.egov.com/apps/me/maine/ag/reportingform (last visited June 16, 2021). The form allows businesses to select one or more of the following descriptors: "loss or theft of device or media," "internal system breach," "insider wrongdoing," "external system breach (hacking)," "inadvertent disclosure," or "other." *Id*.

own employee(s) or agent(s) were directly responsible for the Data Breach, and that the Data Breach was not accidental.[3]

50. The unauthorized, malicious actors were able to gain access to Eye Care's system as a result of Defendants' failure to take the necessary and required minimal steps to secure Plaintiffs' and Class Members' PII and PHI and to exercise reasonable care in the hiring and/or supervision of their employees.

51. Defendants did not begin notifying the individual victims of the Data Breach until late May 2021. For example, Plaintiffs received a letter dated May 28, 2021, from Eye Care notifying them of the Data Breach – ***over four months*** after Eye Care learned of the Data Breach.

52. The notification letters received by Class Members offered them free one-year memberships to Single Bureau Credit Monitoring from TransUnion, a credit reporting agency. *See*, *e.g.*, Sample Notification, Exhibit A. However, this service only monitors fraudulent activity reported to Transunion. Fraudulent activity reported to other reporting bureaus, such as Equifax and Experian, will not be monitored.

Defendants Acknowledge the Harm this Data Breach Has and Will Cause the Victims

53. It is common sense that the criminal(s) that breached Defendants' systems and acquired the victims' PII and PHI did so for the purpose of using that data to commit fraud, theft, and other crimes, or for the purpose of the selling or providing the PII and PHI to other individuals intending to commit fraud, theft, and other crimes. Given that this is the reason such PII and PHI are sought by criminals, it is similarly common sense that Plaintiffs and Class Members have

[3] *See id.*; *see also* Amazon S3 objects overview, AWS, https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingObjects.html (last visited June 16, 2021) (noting that "Amazon S3 resources (for example, buckets and objects) are private by default. You must explicitly grant permission for others to access these resources."). In other words, the Data Breach likely occurred as a direct result of wrongdoing by someone Eye Care "explicitly grant[ed] permission" to.

already suffered injury and face a substantial risk for imminent and certainly impending future injury.

54. Defendants acknowledged the risk faced by victims of the Data Breach. For example, Defendants has offered to provide Class Members with a free one-year membership to credit monitoring services.

55. Similarly, the notifications sent to victims of the Data Breach state: "We urge you to stay alert for incidents of identity theft and fraud, review your account statements, and check your credit reports for shady activity." Defendants apparently acknowledges that Plaintiffs and Class Members may incur costs to obtain credit reports in excess of once per year. *See* Exhibit A (noting that the law only entitles individuals to "one free credit report each year from each of the three major credit reporting bureaus."). Despite urging Class Members to check their credit reports, Defendants have not offered to pay costs associated with Class Members obtaining more than one free credit report each year.

56. Defendants also advised Class Members of their right to obtain a security freeze on their credit reports. Defendants acknowledge that victims exercising their right to obtain a credit freeze will be further inconvenienced and harmed as a result of taking these reasonable steps to prevent future harm. For example, Defendants states that "using a security freeze to take control over who gets access to your credit report may delay or prevent any new loan, credit, mortgage, or any other credit extension request or application you make from being approved timely." *See* Exhibit A.

57. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to

resolve.[4] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[5]

58. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be understated.[6] "A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identity theft: 74 percent of respondents reported feeling stressed, 69 percent reported feelings of fear related to personal financial safety, 60 percent reported anxiety, 42 percent reported fearing for the financial security of family members, and 8 percent reported feeling suicidal."[7]

59. More recently, the FTC released an updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

60. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect customers' PII. The FTC has done this by treating a failure to

---

[4] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), https://www.justice.gov/usao-wdmi/file/764151/download (last visited April 22, 2021).

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

[6] Alison Grace Johansen for NortonLifeLock, *4 Lasting Effects of Identity Theft*, (Mar. 13, 2018), https://www.lifelock.com/learn-identity-theft-resources-lasting-effects-of-identity-theft.html.

[7] *Id.* (citing *Identity Theft: The Aftermath 2016*™, Identity Theft Resource Center (2016) https://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf).

employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. §45.

61. Identity thieves may commit various types of crimes such as, *inter alia*, immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, fraudulently obtaining medical services, and/or using the victim's information to obtain a fraudulent tax refund.

62. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected. Moreover, identify thieves may wait years before using the stolen data.

63. Because the information Defendants allowed to be compromised and taken is of such a durable and permanent quality (*i.e.*, names, Social Security Numbers, dates of birth, and PHI), the harms to Plaintiffs and the Class will continue and increase, and Plaintiffs and the Class will continue to be at substantial risk for further imminent and future harm.

Defendants Knew They Were and Continue to Be Prime Targets for Cyberattacks.

64. Defendants are fully aware of how sensitive the PII and PHI they store and maintain is. They are also aware of how much PII and PHI they collect, use, and maintain from Plaintiffs and Class Members.

65. Defendants knew or should have known that they were ideal targets for hackers and those with nefarious purposes related to sensitive personal and health data. They processed and saved multiple types, and many levels, of PII and PHI through their computer data and storage systems.

66. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiffs' and Class Members' PII and PHI, Defendants assumed certain legal and equitable

duties, and they knew or should have known that they were responsible for the diligent protection of that PII and PHI they collected and stored.

67. Eye Care's notification letters acknowledge the importance of data security and Defendants' duty to Class Members, stating: "We care a lot about the safety of your information," and "[w]e are committed to protecting the privacy and security of your information." *See, e.g.*, Exhibit A.

68. As a large and successful companies, Defendants had the resources to invest in the necessary data security and protection measures. Yet, Defendants failed to exercise reasonable care in the hiring and/or supervision of their employees and agents and failed to undertake adequate analyses and testing of their own systems, adequate personnel training, and other data security measures to avoid the failures that resulted in the Data Breach.

69. The seriousness with which Defendants should have taken its data security is shown by the number of data breaches perpetrated in the healthcare, banking, and retail industries over the past few years.

70. Over 41 million patient records were breached in 2019, with a single hacking incident affecting close to 21 million records.[8] Healthcare breaches in 2019 almost tripled those the healthcare industry experienced in 2018, when 15 million patient records were affected by data breach incidents, according to a report from Protenus and DataBreaches.net.[9]

71. Protenus, a healthcare compliance analytics firm, analyzed data breach incidents disclosed to the U.S. Department of Health and Human Services or the media during 2019, finding

---

[8] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=Over%2041%20million%20patient%20records, close%20to%2021%20million%20records.

[9] *Id.*

that there has been an alarming increase in the number of data breaches of patient privacy since 2016, when there were 450 security incidents involving patient data.[10] In 2019 that number jumped to 572 incidents, which is likely an underestimate, as two of the incidents for which there were no data affected 500 dental practices and clinics and could affect significant volumes of patient records. There continues to be on average at least one health data breach every day.[11]

72. One recent report found that in 2020, healthcare was one of the industries most affected by tracked ransomware incidents.[12]

PII and PHI Are Very Valuable

73. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[13]

74. Consumers rightfully place a high value not only on their PII and PHI, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal

---

[10] *Id*.

[11] *Id*.

[12] Kat Jerich, *Healthcare hackers demanded an average ransom of $4.6 last year, says BakerHostetler*, Healthcare IT News (May 4, 2021), https://www.healthcareitnews.com/news/healthcare-hackers-demanded-average-ransom-46m-last-year-says-bakerhostetler (last visited June 17, 2021).

[13] *The Information Marketplace: Merging and Exchanging Consumer Data*, FTC (Mar. 13, 2001), *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data.

information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[14] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII and PHI to bad actors—would be exponentially higher today.

The PII and PHI at Issue Here is Particularly Valuable to Hackers

75. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers, but credit and debit cards can be cancelled, quickly mitigating the hackers' ability to cause further harm. Instead, PHI and types of PII that cannot be easily changed (such as dates of birth and Social Security Numbers) are the most valuable to hackers.[15]

76. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

77. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies)

[14] Il-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf.

[15] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters., https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited June 17, 2021).

> likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[16]

78. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[17] Victims of the Data Breach, including Plaintiffs, will spend, and already have spent, time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

79. PHI is just as, if not more, valuable than Social Security Numbers. According to a report by the Federal Bureau of Investigation's ("FBI") Cyber Division, healthcare records can be sold by criminals for 50 times the price of stolen Social Security numbers or credit card numbers.[18]

---

[16] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

[17] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

[18] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions/.

A file containing private health insurance information can be bought for between $1,200 and $1,300 ***each*** on the black market.[19]

80. Similarly, the most recent edition of the annual Baker Hostetler Data Security Incident Response Report found that in 2020, hackers in ransomware attacks made an average initial ransomware demand of $4,583,090 after obtaining PHI. In 2020, final payouts to hackers committing ransomware attacks involving PHI averaged $910,335.[20]

81. Companies recognize that PII and PHI are valuable assets. Indeed, PII and PHI are valuable commodities. A "cyber black-market" exists in which criminals openly post stolen PII and PHI on a number of Internet websites. Plaintiffs' and Class Members' compromised PII has a high value on both legitimate and black markets.

82. Some companies recognize PII, and especially PHI, as a close equivalent to personal property. Software has been created by companies to value a person's identity on the black market. The commoditization of this information is thus felt by consumers as theft of personal property in addition to an invasion of privacy.

83. Moreover, compromised health information can lead to falsified information in medical records and fraud that can persist for years as it "is also more difficult to detect, taking twice as long as normal identity theft."[21]

84. Because the information Defendants allowed to be compromised and taken is of such a durable and permanent quality, the harms to Plaintiffs and the Class will continue and

---

[19] Elizabeth Clarke, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents*, SecureWorks (July 15, 2013), https://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents.

[20] Jerich, *supra* n.12.

[21] *See* FBI, *supra* n.18.

increase, and Plaintiffs and Class Members will continue to be at substantial risk for further imminent and future harm.

Defendants' Post-Breach Activity Was (and Remains) Inadequate

85. Immediate notice of a security breach is essential to protect victims such as Plaintiffs and Class Members. Defendants failed to provide such immediate notice, in fact taking more than four months to disclose to victims that there had been a breach, thus further exacerbating the harm to Plaintiffs and Class Members resulting from the Data Breach.

86. Such failure to protect Plaintiffs' and Class Members' PII and PHI, and timely notify of them of the Data Breach, has significant ramifications. The information stolen allows criminals to commit theft, identity theft, and other types of fraud. Moreover, because the data points stolen are persistent—for example, names, dates of birth, and prescription medication data—as opposed to transitory, criminals who access, stole, or purchase the PII and PHI belonging to Plaintiffs and Class Members, do not need to use the information to commit fraud immediately. The PII and PHI can be used or sold for use years later, and often is.

87. Plaintiffs and Class Members are now at a significant risk of imminent and future fraud, misuse of their PII and PHI, and identity theft for many years in the future as a result of the Defendants' actions and the Data Breach. The theft of their PHI is particularly impactful, as many banks or credit card providers have substantial fraud detection systems with quick freeze or cancellation programs in place, whereas the breadth and usability of PHI allows criminals to get away with misuse for years before healthcare-related fraud is spotted.

88. Plaintiffs and Class Members have suffered real and tangible losses, including but not limited to the loss in the inherent value of their PII and PHI, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to

mitigate the costs of injuries realized as a result of discovery in this case, but until recently, kept silent by Defendants.

89. Despite Defendants' egregious failure to protect Plaintiffs' PII and PHI, it has only offered to provide them with trivial compensation or remedy, such as free credit monitoring or identity protection services. Upon information and belief, Defendants similarly did not offer to provide any adequate compensation or remedy to the other victims of the Data Breach (i.e., Class Members).

CLASS ACTION ALLEGATIONS

90. Pursuant to the provisions of Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiffs seek to bring this class action on behalf of themselves and a nationwide class (the "Nationwide Class") defined as:

> **All persons who reside in the United States whose PII and PHI were compromised by the Data Breach.**

91. The Nationwide Class asserts claims against Defendants for negligence, negligence *per se*, and declaratory judgment.

92. Pursuant to Fed. R. Civ. P. 23, Plaintiffs also seek certification of a subclass of Florida residents (the "Florida Subclass") defined as:

> **All individuals residing in Florida whose PII and PHI were compromised by the Data Breach.**

93. The Florida Subclass asserts claims under the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§202-1, *et seq.*

94. Pursuant to Fed. R. Civ. P. 23, Plaintiffs also seek certification of a subclass of Pennsylvania residents (the "Pennsylvania Subclass") defined as:

> **All individuals residing in Pennsylvania whose PII and PHI was compromised by the Data Breach.**

95. The Pennsylvania Subclass asserts claims under the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§202-1, *et seq.*

96. Where appropriate, the Nationwide Class and Subclass shall be referred to collectively as the "Class."

97. The Florida Subclass and the Pennsylvania Subclass will collectively be referred to as the Subclasses.

98. Excluded from the Class are Defendants; officers, directors, and employees of Defendants; any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendants. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

99. Plaintiffs reserve the right to modify and/or amend the Nationwide Class and Subclasses definitions, including but not limited to creating additional subclasses, as necessary.

100. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

101. All Class Members are readily ascertainable in that Defendants have access to addresses and other contact information for all Class Members, which can be used for providing notice to Class Members.

102. ***Numerosity***. The Nationwide Class and Subclasses are so numerous that joinder of all members is impracticable. The Class includes millions of individuals whose personal data was compromised by the Data Breach. Upon information and belief, the Subclasses contain thousands of members.

103. ***Commonality and Predominance***. There are numerous questions of law and fact common to Plaintiffs and the Class that predominate over any questions that may affect only individual Class Members, including the following:

- whether Defendants engaged in the wrongful conduct alleged in this Complaint;
- whether Defendants' conduct was unlawful;
- whether Defendants failed to implement and maintain reasonable systems and security procedures and practices to protect customers' personal data;
- Whether Defendants failed to exercise reasonable care in the hiring of their employees and agents;
- Whether Defendants failed to exercise reasonable care in the supervision of their employees and agents;
- whether Defendants unreasonably delayed in notifying affected customers of the Data Breach;
- whether Defendants owed a duty to Plaintiffs and Class Members to adequately protect their personal data and to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- whether Defendants breached their duties to protect the personal data of Plaintiffs and Class Members by failing to provide adequate data security and failing to provide timely and adequate notice of the Data Breach to Plaintiffs and the Class;
- whether Defendants' conduct was negligent;
- whether Defendants knew or should have known that their computer systems were vulnerable to attack;

- whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach of their systems, resulting in the loss of Class Members' personal data;
- whether Defendants wrongfully or unlawfully failed to inform Plaintiffs and Class Members that they did not maintain computers and security practices adequate to reasonably safeguard customers' personal data;
- whether Defendants should have notified the public, Plaintiffs, and Class Members immediately after they learned of the Data Breach;
- whether Plaintiffs and Class Members suffered injury, including ascertainable losses, as a result of Defendants' conduct (or failure to act);
- whether Plaintiffs and Class Members are entitled to recover damages; and
- whether Plaintiffs and Class Members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

104. ***Typicality***. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all Class Members, had their personal data compromised, breached, and stolen in the Data Breach. Plaintiffs and all Class Members were injured through the uniform misconduct of Defendants, described in this Complaint, and assert the same claims for relief.

105. ***Adequacy***. Plaintiffs and counsel will fairly and adequately protect the interests of the Class. Plaintiffs retained counsel who are experienced in Class action and complex litigation. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of other Class Members.

106. ***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. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiffs and Class Members have been harmed by Defendants' wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct and/or inaction. Plaintiffs know of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendants to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

107. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

108. Particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

(a) Whether Plaintiffs' and Class Members' PII and PHI were accessed, compromised, or stolen in the Data Breach;

(b) Whether (and when) Defendants knew about the Data Breach before they notified Plaintiffs and Class Members and whether Defendants failed to timely notify Plaintiffs and Class Members of the Data Breach;

(c) Whether Defendants owed a legal duty to Plaintiffs and the Class;

(d) Whether Defendants failed to take reasonable steps to safeguard the PII and PHI of Plaintiffs and Class Members;

(e) Whether Defendants failed to adequately monitor their data security systems;

(f) Whether Defendants failed to comply with applicable laws, regulations, and industry standards relating to data security;

(g) Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' PII or PHI secure;

(h) Whether Defendants' adherence to HIPAA regulations, FTC data security obligations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

109. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants, through its uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Defendants continue to maintain their inadequate security practices, retains possession of Plaintiffs' and Class Members' PII and PHI, and has not been forced to change its practices or to relinquish PII and PHI by nature of other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue and appropriate to the Class as a whole.

COUNT I
Negligence

110. Plaintiffs incorporate paragraphs 1-109 of the Complaint as if fully set forth herein.

111. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class, or alternatively, the Subclasses.

112. Plaintiffs and Class Members were required to submit non-public PII and PHI to Defendants and/or their service providers in order to obtain medical service benefits.

113. By collecting, storing, and using Plaintiffs' and Class Members' PII and PHI, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII and PHI it received from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

114. Defendants were required to prevent foreseeable harm to Plaintiffs and Class Members, and therefore had a duty to take reasonable steps to safeguard their sensitive PII and PHI from unauthorized release or theft. More specifically, this duty included: (1) exercising

reasonable care in the hiring, training, and/or supervision of its employees and agents entrusted with access to Plaintiffs' and Class Members' PII and PHI; (2) designing, maintaining, and testing Defendants' data security systems and data storage architecture to ensure Plaintiffs' and Class Members' PII and PHI were adequately secured and protected; (3) implementing processes that would detect an unauthorized breach of Defendants' security systems and data storage architecture in timely and adequate manner; (4) timely acting on all warnings and alerts, including public information, regarding Defendants' security vulnerabilities and potential compromise of the PII and PHI of Plaintiffs and Class Members; (5) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements; and (6) timely and adequately informing Plaintiffs and Class Members if and when a data breach occurred to prevent foreseeable harm to them, notwithstanding undertaking (1)-(5) above.

115. Defendants had a common law duty to prevent foreseeable harm to Plaintiffs and Class Members. The duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate hiring, training, supervision, and security practices of Defendants in their affirmative collection of PII and PHI from Plaintiffs and Class Members. In fact, not only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their PII and PHI because hackers routinely attempt to steal such information for use in nefarious purposes, Defendants knew that it was more likely than not Plaintiffs and Class Members would be harmed as a result.

116. Defendants' duties to use reasonable security measures also arose as a result of the special relationship that existed between they, on the one hand, and Plaintiffs and Class Members, on the other hand. This special relationship, recognized in laws and regulations, arose because Plaintiffs and Class Members entrusted Defendants with their PII and PHI by virtue of receiving

health benefits through Defendants. Defendants alone could have ensured that their security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

117. The injuries suffered by Plaintiffs and Class Members were proximately and directly caused by Defendants' failure to exercise reasonable care in the hiring, training, and/or supervision of their employees and agents, as well as the failure to follow reasonable security standards to protect Plaintiffs and Class Members' PII and PHI.

118. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

119. If Defendants had taken reasonable security measures and/or exercised reasonable care in the hiring, training, and supervision of their employees and agents, data thieves would not have been able to take the personal information of Plaintiffs and Class Members. The policy of preventing future harm weighs in favor of finding a special relationship between Defendants and Plaintiffs and the Class. If companies are not held accountable for failing to take reasonable security measures to protect the sensitive PII and PHI in their possession, they will not take the steps that are necessary to protect against future security breaches.

120. Defendants owed a duty to timely disclose the material fact that Defendants' computer systems and data security practices were inadequate to safeguard users' personal, health, and financial data from theft.

121. Defendants breached these duties through the conduct alleged in the Complaint by, including without limitation, failing to protect the PII and PHI in their possession; failing to maintain adequate computer systems and data security practices to safeguard the PII and PHI in

their possession; allowing unauthorized access to Plaintiffs' and Class Members' PII and PHI; failing to disclose the material fact that Defendants' computer systems and data security practices were inadequate to safeguard the PII and PHI in their possession from theft; and failing to disclose in a timely and accurate manner to Plaintiffs and Class Members the material fact of the Data Breach.

122. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII and PHI would not have been compromised. And as a direct and proximate result of Defendants' failure to exercise reasonable care and use commercially reasonable security measures, the PII and PHI of Plaintiffs and Class Members were accessed by ill-intentioned criminals who could and will use the information to commit identity or financial fraud. Plaintiffs and Class Members face the imminent, certainly impending and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

123. It was foreseeable that Defendants' failure to exercise reasonable care in the hiring, training, and supervision of their employees and agents and to safeguard the PII and PHI in their possession or control would lead to one or more types of injury to Plaintiffs and Class Members. And the Data Breach was foreseeable given the known, high frequency of cyberattacks and data breaches in the healthcare industry.

124. As a proximate result of this conduct, Plaintiffs and the other Class Members suffered damages and will continue to suffer damages in an amount to be proven at trial. Such injuries include those described above, including: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of value of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the

black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach, reviewing bank statements, payment card, statements, insurance statements, and credit reports; expenses and time spent initiating fraud alerts, decreased credit scores and ratings; lost time; other economic harm; and emotional distress.

COUNT II
Negligence *Per Se*

125. Plaintiffs incorporate paragraphs 1-109 of the Complaint as if fully set forth herein.

126. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class, or alternatively, the Subclasses.

127. Plaintiffs and Class Members were required to submit non-public PII and PHI to Defendants and/or their service providers in order to obtain medical service benefits.

128. Pursuant to the FTC Act, 15 U.S.C. §45, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and Class Members.

129. The FTC Act prohibits "unfair . . . practices in or affecting commerce," which the FTC has interpreted to include businesses' failure to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

130. Pursuant to the Gramm-Leach-Bliley Act, Defendants had a duty to protect the security and confidentiality of Plaintiffs' and Class Members' PII. *See* 15 U.S.C. §6801.

131. Pursuant to the Fair Credit Reporting Act ("FCRA"), Defendants had a duty to adopt, implement, and maintain adequate procedures to protect the security and confidentiality of Plaintiffs' and Class Members' PII. *See* 15 U.S.C. §1681(b).

132. Defendants solicited, gathered, and stored PII and PHI of Plaintiffs and Class Members to facilitate transactions which affect commerce.

133. Defendants violated the FTC Act (and similar state statutes), HIPAA, the FCRA, and the Graham-Leach-Bliley Act by failing to use reasonable measures to protect PII and PHI of Plaintiffs and Class Members and not complying with applicable industry standards, as described herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI obtained and stored and the foreseeable consequences of a data breach on Defendants' systems.

134. Defendants' violation of the FTC Act (and similar state statutes) as well as their violations of the FCRA, and the Graham-Leach-Bliley Act constitutes negligence *per se*.

135. Plaintiffs and Class Members are within the class of persons that the FTC Act (and similar state statutes), the FCRA, and the Graham-Leach-Bliley Act were intended to protect.

136. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act (and similar state statutes), as well as the FCRA and the Graham-Leach-Bliley Act were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures caused the same harm as that suffered by Plaintiffs and Class Members.

137. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members have suffered, and continue to suffer, damages arising from the Data Breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

138. Such injuries include those described above, including: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary

loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of value of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach, reviewing bank statements, payment card, statements, insurance statements, and credit reports; expenses and time spent initiating fraud alerts, decreased credit scores and ratings; lost time; other economic harm; and emotional distress.

COUNT III
Declaratory Judgment

139. Plaintiffs incorporate paragraphs 1-109 of the Complaint as if fully set forth herein.

140. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class, or alternatively, on the Subclasses.

141. Under the Declaratory Judgment Act, 28 U.S.C. §2201, *et seq.*, the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

142. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard their users' PII, and whether Defendants is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs and Class Members remain at imminent risk that further compromises of their PII and PHI will occur in the future. This is true even if they (or their healthcare providers) are not actively using Defendants' products or services.

143. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) Defendants continues to owe a legal duty to secure users' PII and PHI and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act;

(b) Defendants continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and Class Members' PII and PHI.

144. The Court also should issue corresponding prospective injunctive relief pursuant to 28 U.S.C. §2202, requiring Defendants to employ adequate security practices consistent with law and industry standards to protect their users' PII and PHI.

145. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendants. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

146. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs at Eye Care, Plaintiffs and Class Members will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

147. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Eye

Care, thus eliminating additional injuries that would result to Plaintiffs, Class Members, and the millions of other Defendants' customers whose PII and PHI would be further compromised.

COUNT IV
Pennsylvania Unfair Trade Practices and Consumer Protection Law
73 P.S. §§202-1, *et seq.*

On Behalf of Plaintiff Bowen and the Pennsylvania Subclass

148. Plaintiffs incorporate paragraphs 1-109 of the Complaint as if fully set forth herein.

149. Plaintiff Bowen brings this claim on behalf of herself and the Pennsylvania Subclass.

150. Defendants engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendants obtained the PII and PHI of Plaintiffs and the Pennsylvania Subclass through trade or commerce directly or indirectly affecting Plaintiffs and the Pennsylvania Subclass and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

151. As alleged herein this Complaint, Defendants engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

(a) failure to implement adequate data security practices to safeguard PII and PHI;

(b) failure to make only authorized disclosures of PII and PHI in their possession; and

(c) failure to disclose that their computer systems and data security practices were inadequate to safeguard PII from theft.

152. Defendants' actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendants engaged in immoral, unethical, oppressive, and

unscrupulous activities that are and were substantially injurious to their current and former customers.

153. In committing the acts alleged above, Defendants engaged in unconscionable, deceptive, and unfair acts and practices by omitting, failing to disclose, or inadequately disclosing to their current and former customers that they did not follow industry best practices for the collection, use, and storage of PII and PHI.

154. As a direct and proximate result of Defendants' conduct, Plaintiff Bowen and the Pennsylvania Subclass have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

155. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff Bowen and the Pennsylvania Subclass have been damaged and are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

156. Also as a direct result of Defendants' knowing violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, Plaintiff Bowen and the Pennsylvania Subclass are entitled to damages as well as injunctive relief, including, but not limited to:

(a) Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

(b) Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

(c) Ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

(d) Ordering that Defendants segment PII and PHI by, among other things, creating firewalls and access controls so that if one area of Defendants' systems are compromised, hackers cannot gain access to other portions of Defendants' systems;

(e) Ordering that Defendants purge, delete, and destroy in a reasonable, secure manner PII and PHI not necessary for their provisions of services;

(f) Ordering that Defendants conduct regular database scanning and securing checks;

(g) Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

(h) Ordering Defendants to meaningfully educate their current and former customers about the threats they face as a result of the loss of their PII and PHI to third parties, as well as the steps Defendants' current and former customers must take to protect themselves; and

(i) Requiring Defendants to thoroughly and regularly evaluate any vendor's or third-party's technology that allows or could allow access to PII and PHI and to promptly migrate to superior or more secure alternatives.

COUNT V
Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. §501.201, *et seq.*

On Behalf of Plaintiff Liang and the Florida Subclass

157. Plaintiffs incorporate paragraphs 1-109 of the Complaint as if fully set forth herein.

158. The FDUTPA prohibits "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce . . ." Fla. Stat. §501.204(1).

159. Defendants advertised, offered, or sold goods and services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

160. Defendants engaged in unfair, unconscionable acts or practices, and unfair or deceptive practices in the conduct of trade and commerce in violation of Fla. Stat. §501.204(1), including by:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Liang's and Florida Subclass members' PII and PHI, which were a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures knowing of the risk of cybersecurity incidents, which were a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Liang's and Florida Subclass members' PII an PHI, including duties imposed by the FTC Act, 15 U.S.C. §45, and Florida's data security statute, Fla. Stat. §501.171(2), which were a direct and proximate cause of the Data Breach;

(d) Misrepresenting that Eye Care would protect the privacy and confidentiality of Plaintiff Liang's and Florida Subclass members' PII and PHI, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that Eye Care would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Laing's and Florida Subclass members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. §45, and Florida's data security statute, Fla. Stat. §501.171(2), which was a direct and proximate cause of the Data Breach;

(f) Omitting, suppressing, and concealing the material fact that Eye Care did not reasonable and adequately security Plaintiff Liang's and Florida Subclass members' PII and PHI; and,

(g) Omitting, suppressing, and concealing the material fact that Eye Care did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Liang's and Florida Subclass members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. §45, and Florida's data security statute, Fla. Stat. §501.171(2).

161. Defendants' misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII and PHI.

162. Had Defendants disclosed to Plaintiff Liang and Florida Subclass members that Eye Care's data systems were not secure and, thus, vulnerable to attack, Defendants would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff Liang's and Florida Subclass members' PII and PHI as part of the services Eye Care provided and for which Plaintiff Liang and Florida Subclass

members paid without advising them that Eye Care's data security measures were insufficient to maintain the safety and confidentiality of Plaintiff Liang's and Florida Subclass members' PII and PHI. Accordingly, Plaintiff Liang and Florida Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

163. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and practices, Plaintiff Liang and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money and property, and monetary and non-monetary damages; losses from fraud and identity theft; costs of credit monitoring and identity theft protection services; time and expenses related to monitoring for fraudulent activity; loss of value of their PII and PHI; and an increased risk of fraud and identity theft.

164. Plaintiff Liang and Florida Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. §501.211; declaratory and injunctive relief; reasonable attorney's fees and costs under Fla. Stat. §501.2105(1); and any other relief that is just and proper.

RELIEF REQUESTED

Plaintiffs, individually and on behalf of the proposed Class, requests that the Court:

1. Certify this case as a class action on behalf of the Nationwide Class and Subclasses, defined above, appoint Plaintiffs as Class representatives, and appoint the undersigned counsel as class counsel;
2. Award declaratory, injunctive, and other equitable relief as is necessary to protect the interests of Plaintiffs and other Class Members;
3. Award restitution; compensatory, consequential, and general damages, including nominal damages as allowed by law in an amount to be determined at trial or by this Court;

4. Award statutory damages to Plaintiffs and Class Members in an amount to be determined at trial or by this Court;
5. Award Plaintiffs and Class Members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;
6. Award Plaintiffs and Class Members pre- and post-judgment interest, to the extent allowable; and
7. Award such other and further relief as equity and justice may require.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable as of right.

Respectfully submitted,

/s/ Stuart A. Davidson
Stuart A. Davidson (0084824)
Dorothy P. Antullis (0890421)
Maxwell H. Sawyer (1003922)
Alexander C. Cohen (1002715)
ROBBINS GELLER RUDMAN & DOWD LLP
120 East Palmetto Park Road
Boca Raton, FL 33432
Phone: (561) 750-3000
Fax: (561) 750-3364
sdavidson@rgrdlaw.com
dantullis@rgrdlaw.com
msawyer@rgrdlaw.com
acohen@rgrdlaw.com

Terence R. Coates (*Pro Hac Vice Forthcoming*)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Joseph M. Lyon (*Pro Hac Vice Forthcoming*)
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 721-1178
jlyon@thelyonfirm.com

Counsel for Plaintiffs and the Class

EXHIBIT A

20/20 Hearing Care NETWORK

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

20/20 Hearing Care Network, Inc. helps manage your hearing benefits for [redacted] **We are writing to tell you about a security incident that may have impacted you as a current or former [redacted] member.** A security incident is an attempted or actual access, use, release, change, or destruction of data by someone that was not given approval to access said data. This letter will tell you what happened and what we are doing to help.

What happened? We realized an unknown person(s) accessed our system and deleted some files on 1/11/21. We do not think there is any actual misuse of your personal or vision/hearing insurance information, but we don't know for sure. A cybersecurity firm looked into the incident for us and could not tell which files were seen or deleted by the unknown person(s). Thus, we looked at all the information on the system that could have been seen or deleted to see if your information was involved.

What information was involved? Your Social Security number, member identification number, date of birth and health insurance information may have been seen or accessed before being deleted. This information is called your personal information or protected health information (PHI). It tells others about you and is part of your identity.

What we are doing. We care a lot about the safety of your information. We have:

- Looked into what caused this incident to occur.
- Taken steps to reduce the risk this will happen again, like:
  - Resetting passwords.
  - Telling the FBI about the problem. They are investigating it.
  - Sending letters to everyone whose information may be involved, including you.
- Reviewed and started making our policies and procedures stronger.

We are committed to protecting the privacy and security of your information.

What you can do. Please read the "Steps You Can Take to Help Protect Your Information" pages with this letter. They give:

- Tips to help you keep your identity safe, like looking over health account statements and credit reports for things you didn't buy.
- The list of agencies to whom you can report issues of bad payments.
- Steps on how to sign up for free credit monitoring services.

Do you need help? Call 1-833-580-2416 toll free Monday through Friday, 8:00 a.m. to 5:00 p.m. Central Time if you have questions.

Sincerely,

20/20 Hearing Care Network, Inc.

Steps You Can Take to Help Protect Your Information

Enroll in Free Credit Monitoring

We are providing you with access to **Single Bureau Credit Monitoring*** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your TransUnion credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft, as well as a $1,000,000 insurance reimbursement policy.

To enroll in Credit Monitoring services at no charge, please log on to **idforces.com** and follow the instructions provided. When prompted, please provide the following unique code to receive services: **<<Activation Code>>.** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 5:00 p.m. Central time, Monday through Friday. Please call the help line at 1-833-580-2416 and supply the fraud specialist with your unique code listed above. To extend these services, enrollment in the monitoring services described above is required.

Check Your Accounts

We urge you to stay alert for incidents of identity theft and fraud, review your account statements, and check your credit reports for shady activity. Under U.S. law, you are eligible for one free credit report each year from each of the three major credit reporting bureaus. To order your free credit report, visit annualcreditreport.com or call toll-free 877-322-8228. You may also reach out to the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a security freeze on your credit report. The security freeze will stop a consumer reporting agency from giving out personal or financial information in your credit report without your consent. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Note: using a security freeze to take control over who gets access to your credit report may delay or prevent any new loan, credit, mortgage, or any other credit extension request or application you make from being approved timely. Under federal law, you cannot be charged to place or lift a security freeze on your credit report. If you wish to place a security freeze, please reach out to these major consumer reporting agencies:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
888-397-3742	888-909-8872	800-685-1111
experian.com/freeze	transunion.com/credit-freeze	equifax.com/personal/credit-report-services

To request a security freeze, you will need to provide these items:

1. Your full name with middle initial and suffix (Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. The addresses where you have lived over the last five years, if you have moved
5. Proof of current address, such as a current utility bill or telephone bill
6. A clear photocopy of a government-issued identification card (state driver's license or ID card, military ID, etc.)
7. If you are a victim of identity theft, show a copy of either the police or investigative report or complaint to a law enforcement agency about identity theft

Instead of a security freeze, you have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Businesses are required to take steps to verify a consumer's identity before extending new credit once they see a fraud alert on a credit file. If you are a victim of identity theft, you are eligible for an extended fraud alert. This is a fraud alert lasting seven years. If you wish to place a fraud alert, please reach out to any one of these agencies:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
888-397-3742	800-680-7289	888-766-0008
experian.com/fraud	transunion.com/fraud-victim-resource/place-fraud-alert	equifax.com/personal/credit-report-services

More Information

You can learn more about identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by reaching out to:

- The consumer reporting agencies.
- The Federal Trade Commission at: 600 Pennsylvania Ave. NW, Washington, DC 20580, identitytheft.gov, 877-ID-THEFT (877-438-4338); TTY: 866-653-4261.
  - The FTC also urges those who learn their information has been misused to file a complaint with them. Reach out to the FTC for steps to file such a complaint.
- Your state Attorney General.

You have the right to file a police report if identity theft or fraud ever happen to you. Note: to file a report with law enforcement for identity theft, you will need to give some proof you have been a victim. Also, you must report cases of known or presumed identity theft to law enforcement and your state Attorney General.

All U.S. Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580, consumer.gov/idtheft, 877-IDTHEFT (877-438-4338), TTY: 866-653-4261.

California Residents: Visit the California Office of Privacy Protection (oag.ca.gov/privacy) for more information to protect yourself against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Ave., Ste. 118, Frankfort, KY 40601**,** ag.ky.gov, 502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, 888-743-0023 or 410-528-8662.

New Mexico Residents: You have rights under the Fair Credit Reporting Act, such as the rights to:

- Be told if information in your credit file has been used against you.
- Know what is in your credit file.
- Ask for your credit score.
- Dispute lacking or wrong information.

Also, under the Fair Credit Reporting Act:

- The consumer reporting agencies must correct or delete wrong, lacking, or unverifiable information.
- The consumer reporting agencies may not report outdated bad information.
- Access to your file is limited.
- You must give your consent for credit reports to be given to employers.
- You may limit "prescreened" credit and insurance offers you get based on information in your credit report.
- You may seek damages from a violator.

You may have more rights under the Act not reviewed here. Identity theft victims and active duty military personnel have more specific rights under to the Act. You can review your rights under the Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

New York Residents: Contact the Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 800-771-7755; https://ag.ny.gov.

North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 919-716-6400, 877-566-7226 (toll free within NC).

Oregon Residents: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, www.doj.state.or.us, 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 S. Main St., Providence, RI 02903, www.riag.ri.gov, 401-274-4400. Under Rhode Island law, you have the right to get any police report filed about this incident. There are 60 Rhode Island residents impacted by this incident.

Washington D.C. Residents: Reach the Office of Attorney General for the District of Columbia at: 400 6th St. NW, Washington, DC 20001; 202-442-9828; https://oag.dc.gov.