UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

Case No. 21-CV-61275-RAR

WENSTON DESUE, Individually and as Legal Guardian of N.D. and M.D., and All Others Similarly Situated,

Plaintiffs,

vs.

20/20 EYE CARE NETWORK, INC., *et al.*,

Defendants.

AND ALL CONSOLIDATED ACTIONS.

CLASS ACTION

CONSOLIDATED WITH:
No. 21-cv-61292
No. 21-cv-61302
No. 21-cv-61357
No. 21-cv-61406
No. 21-cv-61755

JURY TRIAL DEMANDED

SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Stephany Alcala; Benjamin J. Liang; Amber Lowe, on behalf of herself and her minor children C.B., K.B., M.B., and G.M.; David Runkle; and Suzanne Johnson (collectively, "Plaintiffs"), individually and on behalf of all other persons similarly situated, by and through their attorneys, upon personal knowledge as to themselves and their own acts and experiences, upon investigation of their counsel, and upon information and belief as to all other matters, allege as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this Second Amended Consolidated Class Action Complaint against Defendants 20/20 Eye Care Network, Inc. ("20/20 Eye Care") and iCare Acquisition, Inc. ("iCare") (collectively "Defendants"), to hold Defendants accountable for the harm they caused to Plaintiffs and over 3.2 million similarly situated persons, including minors ("Class Members"), from their failure to properly secure and safeguard current and former patients' sensitive personally

identifiable information ("PII"), including their names, dates of birth, Social Security numbers, and protected health information ("PHI"), such as patients' member identification numbers and health insurance information.

2. The full extent of the types of sensitive personal information, the scope of the breach, and the root cause of the Data Breach is all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation.

3. On January 11, 2021, Defendant 20/20 Eye Care was alerted to suspicious activity in its Amazon Web Services ("AWS") cloud storage environment. Over a month later, 20/20 Eye Care confirmed that, in fact, data in cloud storage locations (known as S3 buckets) storing Plaintiffs' and Class Members' PII and PHI had been accessed, that data in those S3 buckets hosted on AWS environment had been "removed" and all data in those S3 buckets was deleted (the "Data Breach").[1]

4. In or about June 2021, Plaintiffs received letters dated May 28, 2021, similar to a letter 20/20 Eye Care submitted to the Office of the Maine Attorney General.[2] The notice letters stated that in January 2021, PII and PHI that were on 20/20's systems had been illegally exposed to unknown person(s). The notifications revealed that unauthorized person(s) "removed" data and "accessed [20/20's] system and deleted some files."[3]

---

[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 Mar. 29, 2022). "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 Mar. 29, 2022).

[2] *See Data Breach Notifications*, Me. Att'y. Gen., attached as Ex. 1.

[3] *Id.*

5. The Data Breach occurred because Defendants failed to implement adequate, reasonable, and industry-mandated cyber-security procedures and protocols to protect the PII and PHI of Plaintiffs and Class Members. Indeed, the deficiencies in Defendants' data security protocols and practices were so significant that unauthorized person(s) were able to access, view, remove or download, and then delete patient data.

6. Defendants did not adequately safeguard and protect Plaintiffs' PII and PHI, and now Plaintiffs, along with millions of other Class Members, are the victims of a significant Data Breach that, among other harms, puts them at a substantially increased risk of identity fraud, which will negatively impact them, including some of their minor or dependent children, for years.

7. Defendants are responsible for this Data Breach through their failure to implement and maintain adequate and reasonable data security safeguards, their failure to comply with industry-standard data security practices, and their failure to comply with federal and state laws and regulations governing data security and privacy of PII and PHI.

8. Despite their role in managing so much sensitive and personal PII and PHI, Defendants failed to timely recognize and detect the unauthorized access and use of their systems, and further failed to timely recognize that substantial amounts of data had been compromised.

9. Defendants failed to, among other things, timely detect that a criminal third party had accessed their computer data and storage systems, failed to notice that massive amounts of data were compromised, and failed to take any steps to investigate the red flags that should have warned Defendants that their systems were not secure and were being targeted and attacked. Had Defendants properly maintained and monitored their information technology infrastructure and denied or circumvented access to that infrastructure to all potential and active threats, Defendants would have discovered the invasion sooner – and/or prevented it altogether.

10. 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"). Defendants were and are still required to maintain the security and privacy of the PII and PHI entrusted to them. When Plaintiffs and Class Members provided their PII and PHI, Defendants and their agents were required to comply with these obligations to keep Plaintiffs' PII and PHI secure and safe from unauthorized access, to use this information for business purposes only, and to make only authorized disclosures of this information.

11. 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.

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

13. As a result of Defendants' failures, the PII and PHI of Plaintiffs and Class Members were accessed and downloaded by one or more malicious actors. 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.

14. Plaintiffs' and Class Members' injuries were exacerbated by the delay in informing and notifying Plaintiffs and Class Members of the Data Breach and the theft of their PII and PHI. Plaintiffs and Class Members were unable to take actions to protect themselves and attempt to mitigate the harm until they received notice.

15. Plaintiffs and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their valuable 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 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; (e) damages to and diminution in value of their personal data; (f) invasion of privacy; (g) actual damages in the form of the difference in value between the services that should have been delivered and the services that were actually delivered; 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 fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII and PHI.

16. 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.

17. Accordingly, Plaintiffs, on behalf of themselves and Class Members, assert claims for negligence, negligent supervision, and violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§501.201, *et seq*. ("FDUTPA"). Plaintiffs seek injunctive relief and all other relief as authorized in equity or by law.

THE PARTIES

Defendant 20/20 Eye Care

18. Defendant 20/20 Eye Care is a Florida corporation with its principal place of business in Ft. Lauderdale, Florida.

19. 20/20 Eye Care is a managed vision care company that offers third-party administrative services. It contracts with optometrists, ophthalmologists, ambulatory surgical centers, and retail vision centers to provide a full spectrum of eye care needs.

20. 20/20 Eye Care acts as a third-party plan administrator, assisting insurance companies and patients with claims processing, credentialing of professionals, and linking patients with in-network providers, management utilization services, and network leasing.

Defendant iCare

21. Defendant iCare is a Delaware corporation with its principal place of business in Miami, Florida.

22. Upon information and belief, in September 2020, Defendant iCare, backed by private equity firm Pine Tree Equity IV, LP, acquired Defendant 20/20 Eye Care and, in whole or in part, controls 20/20 Eye Care in providing integrated eye care as both Florida's largest managed service provider and the largest ophthalmology and optometry provider with over 55 owned locations.

23. 20/20 Eye Care was originally under common ownership with 20/20 Hearing Care, a company that manages a network of audiologists to refer managed care members to, acting as a middleperson between managed care plans and their members. The two companies used a shared data platform. Defendant iCare acquired 20/20 Eye Care prior to the Data Breach, but it did not acquire 20/20 Hearing Care. The data platform stayed with 20/20 Eye Care, and 20/20 Eye Care provides services on behalf of 20/20 Hearing Care under a services agreement that continued following iCare's acquisition of 20/20 Eye Care. 20/20 Eye Care and 20/20 Hearing Care shared and stored patients' PII and PHI, including Plaintiffs' and Class Members' PII and PHI, in the same platform, which was compromised in the Data Breach.

24. Because Defendants 20/20 Eye Care and iCare owned, operated, and managed the database shared with 20/20 Hearing Care, Defendants were responsible for the failures in data security and employee supervision that resulted in the Data Breach; therefore, Defendants are also

liable for the breach of data provided by patients of 20/20 Hearing Care regardless of who provided the notice of the Data Breach.

Plaintiff Stephany Alcala

25. Plaintiff Stephany Alcala is a citizen of Florida residing in Miami, Florida.

26. Plaintiff Alcala is very careful about sharing her PII and PHI, and she has never knowingly transmitted her PII and PHI unencrypted over the internet or any other unsecured source. Plaintiff Alcala stores any and all documents containing her PII and PHI in a safe and secure location, and she destroys any documents she receives in the mail that may contain any information that could be used to compromise her financial accounts, commit fraud, and steal her identity. Plaintiff Alcala has sought treatment for eye issues and has seen medical providers related to those issues over the years in Florida. She provided those providers with her PII and PHI in order to receive treatment services prior to the Data Breach.

27. Plaintiff Alcala received 20/20 Eye Care's May 28, 2021 Notice of Data Breach on or about that date. The notice informed her that Defendants' systems had been compromised and that her name, Social Security number, date of birth, member identification number, and health insurance information may have been viewed, accessed, and deleted in the Data Breach.

28. Upon information and belief, Plaintiff's PII and PHI was targeted, accessed, and downloaded by the third-party criminal actors in the Data Breach.

29. As a result of the Data Breach, Plaintiff Alcala faces a substantial risk of imminent identity, financial, and health fraud and theft—both now and for years.

30. Moreover, Plaintiff Alcala has experienced actual identity fraud. In approximately June 2021, Plaintiff Alcala had at least four hard inquiries on her credit report from four entities with which she has no prior relationship.

31. Additionally, after the Data Breach, an unknown third party applied for a personal loan in Plaintiff Alcala's name at Penn Fed Credit Union.

32. Upon information and belief, these acts of identity fraud are related to her compromised PII and PHI in the Data Breach.

33. In response to the Data Breach and fraudulent activity, Plaintiff Alcala made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services; and at an annual $140 cost she purchased UltraSecure+Credit from Identity Force, which she will need to maintain for years to mitigate any further fraud attempts. This is valuable time Plaintiff Alcala otherwise would have spent on other activities, including but not limited to work, recreation, and the private enjoyment of life.

34. Plaintiff Alcala is deeply concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

35. Plaintiff Alcala suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of her PII and PHI, a form of property that Defendants obtained from Plaintiff Alcala; (b) violation of her privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) time and money spent mitigating the risk and addressing fraudulent activity.

36. As a result of the Data Breach, Plaintiff Alcala anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

Plaintiff Benjamin Liang

37. Plaintiff Benjamin Liang is a natural person and a resident of Sunrise, Florida.

38. Plaintiff Liang is very careful about sharing his PII and PHI, and he has never knowingly transmitted his PII and PHI unencrypted over the internet or any other unsecured source.

39. Plaintiff Liang stores any and all documents containing his PII and PHI in a safe and secure location, and he destroys any documents he receives in the mail that may contain any information that could be used to compromise his financial accounts, commit fraud, and steal his identity.

40. Prior to the Data Breach, 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.

41. Plaintiff Liang received 20/20 Eye Care's May 28, 2021 Notice of Data Brach on or about that date. The letter explained that Defendants' systems had been compromised and that Plaintiff's name, date of birth, Social Security number, member identification number, and health insurance information may have been viewed, accessed, or deleted in the Data Breach.

42. Upon information and belief, Plaintiff's PII and PHI was targeted, accessed, and downloaded by the third-party criminal actors in the Data Breach.

43. 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 years.

44. 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.

45. Furthermore, Plaintiff Liang has also experienced an increased amount of robocalls since the Data Breach adding nuisance, annoyance and loss of time and attention.

Plaintiffs Amber Lowe and minor children C.B., K.B., M.B., and G.M.

46. Plaintiff Amber Lowe is an individual who resides in Callahan, Florida.

47. Plaintiff Lowe is very careful about sharing her and her children's PII and PHI and has never knowingly transmitted her or her children's PII and PHI unencrypted over the internet or any other unsecured source.

48. Plaintiff Lowe stores any and all documents containing her and her minor children's PII and PHI in a safe and secure location, and she destroys any documents she receives in the mail that may contain any information that could be used to compromise her and her minor children's financial accounts, commit fraud, and steal her and her minor children's identity.

49. Plaintiff Lowe is the legal guardian of Plaintiffs C.B., K.B., M.B., and G.M., minor patients of 20/20, who also reside in Callahan, Florida.

50. Prior to the Data Breach, Plaintiff Lowe sought eye care treatment from medical providers in Florida for herself and her four children. Plaintiff gave those providers both her and her children's PII and PHI in order to receive treatment services.

51. Plaintiff Lowe received 20/20 Eye Care's May 28, 2021 Notice of Data Breach on or about that date. The letter explained that Defendants' systems had been compromised and that Plaintiffs Lowe, C.B., K.B., M.B., and G.M.'s names, dates of birth, Social Security numbers, member identification numbers, and health insurance information may have been viewed accessed or deleted in the Data Breach.

52. Upon information and belief, the PII and PHI of Plaintiffs Lowe, C.B., K.B., M.B., and G.M. was targeted, accessed, and downloaded by the third-party criminal actors in the Data Breach.

53. As a result of the Data Breach, Plaintiffs Lowe, C.B., K.B., M.B., and G.M. each face a substantial risk of imminent identity, financial, and health fraud and theft—both now and for years.

54. Following the Data Breach, Plaintiff Lowe experienced actual identify fraud. On or about March 8, 2021, Plaintiff Lowe was attempting to renew her application for benefits with the Florida Department of Children and Families when she was alerted that on January 17, 2021, an unauthorized third-party had opened an account with the Florida Department of Economic Opportunity.

55. Furthermore, Plaintiff Lowe was informed that someone had created an application for unemployment benefits with the Department of Economic Opportunity using Plaintiff Lowe's name, Social Security number, and former address. The identity thief successfully received approximately four payments from the Department of Economic Opportunity in Plaintiff Lowe's name.

56. Upon information and belief, these acts of identity fraud stem from her compromised PII and PHI in the Data Breach.

57. Upon learning that she was a victim of identity theft, Plaintiff Lowe contacted the Jacksonville Sheriff's Office and filed a police report. At the instruction of the police, Plaintiff Lowe placed a freeze on her credit reports. Plaintiff Lowe also directly contacted the Department of Economic Opportunity in an attempt to resolve the issue.

58. At the time, Plaintiff Lowe was unaware that her PII and PHI had been compromised approximately two months prior in the Data Breach.

59. As a result of the fraudulent unemployment benefit application, Plaintiff Lowe was unable to successfully renew her benefits with the Department of Children and Families, which include food assistance for her and her minor children, Plaintiffs C.B., K.B., M.B., and G.M.

60. Due to the fraudulent unemployment benefit application made using her PII, Plaintiff Lowe and her children were without benefits from the Department of Children and Families, including food assistance benefits, for two months while the Department of Children and Families investigated the fraudulent unemployment benefit application.

61. In addition to suffering the loss of financial and food assistance benefits for two months, Plaintiff Lowe has suffered significant stress attempting to convince the Department of Children and Families that she did not unlawfully apply for unemployment benefits. Plaintiff Lowe experienced, among other things, fear of losing her job, fear of criminal repercussions, and fear of being unable to provide her children with food and basic life necessities.

62. Furthermore, Plaintiff Lowe has spent increased time reviewing her financial statements to determine whether there has been fraudulent activity on her accounts. 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.

Plaintiff David Runkle

63. Plaintiff David Runkle is a natural person and a resident of Wilton Manors, Florida.

64. Plaintiff Runkle is very careful about sharing his PII and PHI, and he has never knowingly transmitted his PII and PHI unencrypted over the internet or any other unsecured source.

65. Plaintiff Runkle stores any and all documents containing his PII and PHI in a safe and secure location, and he destroys any documents he receives in the mail that may contain any information that could be used to compromise his financial accounts, commit fraud, and steal his identity.

66. Plaintiff Runkle has sought medical care and treatment through Simply Healthcare Plans, Inc. since 2018. He provided Simply Healthcare with his PII and PHI in order to receive medical care and treatment services.

67. Plaintiff Runkle received 20/20 Eye Care's May 28, 2021 Notice of Data Brach on or about that date. The letter explained that Defendants' systems had been compromised and that Plaintiff's name, date of birth, Social Security number, member identification number, and health insurance information may have been viewed, accessed, or deleted in the Data Breach.

68. Upon information and belief, Plaintiff's PII and PHI was targeted, accessed, and downloaded by the third-party criminal actors in the Data Breach.

69. As a result of the Data Breach, Plaintiff Runkle faces a substantial risk of future identity, financial, and health fraud and theft—both now and for years.

70. Plaintiff Runkle is an English-speaking resident of Florida, who does not speak or read Spanish. The May 28, 2021 Data Breach notice letter Plaintiff Runkle received was entirely in Spanish and provided Plaintiff Runkle a number to call for more information concerning the Data Breach. Plaintiff called this number soon after receiving it and requested information about the Data Breach in English and was notified that another letter in English could be sent to his residence in six to eight weeks. Subsequently, on June 9, 2021, four separate bank accounts in Plaintiff Runkle's name were opened at SunTrust Bank without his knowledge or authority. A

few days later, on June 12, 2021, based on fraudulent activity identified by SunTrust Bank, the four bank accounts were closed, and Plaintiff Runkle was notified.

71. Upon information and belief, these acts of identity fraud stem from Plaintiff's compromised PII and PHI in the Data Breach.

72. In addition, the Data Breach has cost Plaintiff a significant loss of time. To date, Plaintiff Runkle has spent countless hours on the phone attempting to cure these nefarious criminal activities, which used his credit and Social Security number to open unauthorized bank accounts in his name. In response to the four SunTrust Bank account activity, Plaintiff Runkle opened a police incident report with the Wilton Manors Police Department on June 16, 2021 to investigate the unauthorized banking activity in his name at SunTrust Bank.

73. Furthermore, Plaintiff Runkle has spent increased time reviewing his financial statements to determine whether there has been any additional fraudulent activity on his accounts. He will continue to spend additional time every day to review his statements due to the increased risk of identity theft posed by the unlawful disclosure of his PII and PHI.

74. Plaintiff Runkle has also spent several hours changing various account passwords, speaking on the phone about the Data Breach with entities such as his insurance providers, and researching the Data Breach. He also plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach.

Plaintiff Suzanne Johnson

75. Plaintiff Suzanne Johnson is a natural person and a resident of Pinellas County, Florida.

76. Plaintiff Johnson is very careful about sharing her PII and PHI, and she has never knowingly transmitted her PII and PHI unencrypted over the internet or any other unsecured source.

77. Plaintiff Johnson stores any and all documents containing her PII and PHI in a safe and secure location, and she destroys any documents she receives in the mail that may contain any information that could be used to compromise her financial accounts, commit fraud, and steal her identity.

78. Plaintiff Johnson has sought treatment from Defendants' network of medical providers over the years in Florida. She provided those providers with her PII and PHI in order to receive treatment services.

79. Plaintiff Johnson received 20/20 Eye Care's May 28, 2021 Notice of Data Brach on or about that date. The letter explained that Defendants' systems had been compromised and that Plaintiff's name, date of birth, Social Security number, member identification number, and health insurance information may have been viewed, accessed, or deleted in the Data Breach.

80. Upon information and belief, Plaintiff's PII and PHI was targeted, accessed, and downloaded by the third-party criminal actors in the Data Breach.

81. As a result of the Data Breach, Plaintiff Johnson faces a substantial risk of imminent identity, financial, and health fraud and theft—both now and for years.

82. Since learning about the Data Breach, Plaintiff Johnson continues to worry about the Data Breach's impact on her PII and PHI and is fearful that she will be required to continue zealously monitoring her identity, credit, and other PII and PHI for perhaps the rest of her life.

83. Plaintiff Johnson has spent increased time reviewing her financial statements and credit on a daily basis to determine whether there has been any fraudulent activity on her accounts. For example, as a result of the Data Breach, she now spends approximately half an hour per day to check her financial accounts. She will continue to spend additional time every week to review

her statements and credit due to the increased risk of identity theft posed by the unlawful disclosure of her PII and PHI.

84. Furthermore, Plaintiff Johnson has also experienced an increased number of phishing calls and emails since the Data Breach that have caused additional nuisance, annoyance, and loss of time and attention.

JURISDICTION & VENUE

85. 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, Plaintiffs, many absent Class Members,[4] and Defendants are citizens of different states.

86. This Court has general personal jurisdiction over 20/20 Eye Care because its principal place of business is located in this district at 2900 W. Cypress Creek Road, Suite 4, Fort Lauderdale, Florida 33309.

87. This Court has general personal jurisdiction over iCare because its principal place of business is located in this district at 1515 Sunset Drive, Suite 32, Miami, Florida 33143.

88. Venue is proper in this district under 28 U.S.C. §§ 1391(a)(1), 1391(b)(1), 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, Defendants conduct substantial business in this district, and Defendants all reside in this district. On information and belief, Plaintiffs' and Class Members' PII and PHI was transmitted to and by Defendants and input into their network within the district. Defendants are based in this district, are believed to maintain Plaintiffs' and Class Members' PII

[4] While Defendants serve Floridians, persons outside Florida were impacted, including 221 residents of Maine. Me. Att'y Gen. Notice, *supra* n.2, Ex. 1.

and PHI in the district and the harm caused to Plaintiffs and Class Members emanated from this district.

FACTUAL ALLEGATIONS

Defendants Acquire, Collect, and Maintain Plaintiffs' and Class Members' PII and PHI.

89. Insurers contract with 20/20 Eye Care to provide an allegedly more efficient process by which patient claims may be processed. 20/20 Eye Care also "contract[s] with optometrists, ophthalmologists, ambulatory surgical centers, and retail vision centers to provide a full spectrum of eye care needs."[5]

90. In connection with procuring and providing health care services to patients such as Plaintiffs and Class Members, 20/20 Eye Care acquires, collects, and maintains a massive amount of PHI and other PII of patients.

91. Upon information and belief, 20/20 Hearing Care also stores patient PII and PHI in the database owned, controlled, operated, and improperly secured by 20/20 Eye Care pursuant to a management services agreement, whereby 20/20 Eye Care services claims and holds patient PII and PHI on behalf of 20/20 Hearing Care.

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

93. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI. Defendants were required to keep Plaintiffs' and Class

[5] 20/20 EyeCare Network, http://our2020.com/ (last visited Mar. 29, 2022).

Members' PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach

94. On January 11, 2021, 20/20 Eye Care was alerted to suspicious activity in its Amazon AWS cloud storage environment. It later discovered that certain S3 buckets hosted in AWS had been accessed, data in those buckets had been downloaded, and then all data in those S3 buckets was deleted.

95. In late February 2021, 20/20 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, including patients of 20/20 Hearing Care.

96. Defendants then provided notice to various state Attorneys General, including the Maine Attorney General[6] and the California Attorney General, that described the Data Breach as "insider wrongdoing." This description indicates that Defendants' own employee(s) or agent(s) were directly responsible for the Data Breach and that the Data Breach was not accidental.[7] The Maine Attorney General letter provided:

> On January 11, 2021, 20/20 was alerted to suspicious activity in its Amazon Web Services ("AWS") environment. In response, access credentials to the

[6] Me. Att'y Gen. Notice, *supra* n.2, Ex. 1. The Maine Attorney General requires that businesses suffering a data breach involving residents of Maine must submit notice to the Maine Attorney General on a form provided by the Maine Attorney General. *See* Maine Security Breach Reporting Form, Me. Att'y Gen.'s office. 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*

[7] Me. Att'y Gen. Notice, *supra* n.2, Ex. 1; *see also* Amazon S3 objects overview, AWS, https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingObjects.html (last visited Mar. 29, 2022) (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 20/20 "explicitly grant[ed] permission" to.

> AWS environment were reviewed and deactivated/reset, and other responsive security measures were immediately put into place. In response to the deletion event, 20/20 promptly notified the FBI. After reviewing available evidence, the investigation determined that on January 11, 2021, data was potentially removed from the S3 buckets hosted in AWS and all the data in the S3 buckets was then deleted. The forensic investigation continued, and in late February, 20/20 determined the data could have potentially included information about some or all health plan members for whom it had records.
>
> At this time, 20/20 has notified the relevant health plans believed to have been impacted as a result of this event. Subsequently, an exhaustive review to determine what specific data may be at risk and to whom that information relates was conducted. Upon completion of the review and verification of the data, 20/20 notified individuals and relevant regulators as soon as possible.
>
> The information that could have been subject to unauthorized access includes name, address, Social Security number, member identification number, date of birth, and health insurance information.[8]

97. The letters to the Maine Attorney General and California Attorney General also enclosed a sample template Data Breach notice letter from 20/20 Hearing Care, which explained the Data Breach, in relevant part by setting forth:

> ***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 detected. This information is called your personal information or protected health information (PHI). It tells others about you and is part of your identity.[9]

---

[8] Me. Att'y Gen. Notice, *supra* n.2, Ex. 1.

[9] *See, e.g.*, Me. Att'y Gen. Notice, *supra* n.2, Ex. 1 (Ex. A); *see also* Cal. Att'y Gen. Letter, https://oag.ca.gov/system/files/20-20%20-%20Sample%20Letter.PDF (last visited Mar. 29, 2022).

98. The template letter "urge[d]" Class Members "to stay alert for incidents of identity theft and fraud, review [their] account statements, and check [their] credit reports for shady activity." It further instructed that Class members could learn more information on "identity theft, fraud alerts, security freezes, and the steps [they] can take to protect [themselves]" by contacting, *inter alia*, their state Attorneys General, including in California, Kentucky, Maryland, New Mexico, New York, North Carolina, Oregon, Rhode Island, and Washington D.C.[10]

99. Defendants began notifying the individual victims of the Data Breach in late May 2021. Plaintiffs Alcala, Liang, and Lowe received Data Breach notice letters from 20/20 Eye Care dated May 28, 2021, notifying them of the Data Breach.

100. Plaintiffs Runkle and Johnson received a Data Breach notice letter from 20/20 Hearing Care, also dated May 28, 2021.

101. The letters, which were substantially the same as the template letter, stated that that there had been "a privacy issue involving some of your health information." They "encourage[d] [Plaintiffs and Class Members] to remain vigilant against incidents of identity theft and fraud, to review [their] account statements, and to monitor [their] credit report for suspicious activity."

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

[10] Me. Att'y Gen. Notice, *supra* n.2, Ex. 1 (Ex. A).

103. This is wholly inadequate because victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft. Moreover, Defendants' offer does not address any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII and PHI, including private and sensitive medical information.

104. The letter also advised Plaintiffs and Class Members they had the right to obtain "one free credit report annually from each of the three major credit reporting bureaus." Despite instructing Plaintiffs to "monitor [their] credit reports," Defendants did not offer to pay costs associated with Plaintiffs obtaining more than "one free credit report annually[.]"

105. Furthermore, Defendants' providing information on how to sign up for free credit monitoring squarely places the burden on Plaintiffs and Class Members, rather than Defendants, to investigate and protect themselves from Defendants' tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiffs and Class Members in credit monitoring services upon discovery of the Data Breach, Defendant merely sent instructions "offering" the services to affected patients recommending they sign up for the services.

106. The Data Breach notices also advised Plaintiffs and Class Members of their right to obtain a security freeze on their respective credit reports. 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."

107. Based on Defendants' urging Plaintiffs and Class Members to take these mitigating actions immediately, it is abundantly clear that the perils from the Data Breach are real and concrete, and not hypothetical or attenuated.

108. Despite all of the publicly available knowledge of the continued compromises of PII and PHI, Defendants' approach to maintaining the privacy of Plaintiffs' and Class Members' PII and PHI was inadequate, unreasonable, reckless, and negligent. This is evidenced by Defendants' Data Breach notice, in which Defendants stated in response to the Data Breach that they "[r]eviewed and started making our policies and procedures stronger." Implied in Defendants' statement is an admission that Defendants' technical and cybersecurity capabilities were inadequate, which resulted in the Data Breach and the divulgence of Plaintiffs' and Class Members' PII and PHI.

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

109. 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.

110. 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.[11]

111. Defendants knew or should have known that they were ideal targets for hackers and others with nefarious purposes related to sensitive personal identifying and health information.

[11] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters. (July 21, 2020), 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 Mar. 29, 2022).

20/20 processed and saved multiple types, and many levels, of PII and PHI through its computer data and storage systems.

112. Indeed, the Federal Bureau of Investigation ("FBI") has expressed concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry, like Defendants, that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[12]

113. The American Medical Association ("AMA") has also warned healthcare companies like Defendants about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[13]

114. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[14]

---

[12] Jim Finkle, *FBI warns healthcare firms that they are targeted by hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820, (last visited Mar. 29, 2022).

[13] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AMA (Oct. 4, 2016), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals, (last visited Mar. 29, 2022).

[14] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf, (last visited Mar. 29, 2022).

115. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. According to the 2019 HIMSS Cybersecurity Survey, 82% of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[15] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[16]

116. As major healthcare service administrator, Defendants knew, or should have known, the importance of safeguarding the patients' PII and PHI entrusted to it and of the foreseeable consequences if that data was disclosed. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

117. 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.

118. Defendants' notification letters acknowledge the importance of data security and its 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."

---

[15] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Mar. 29, 2022).

[16] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, Chief Healthcare Executive (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks, (last visited Mar. 29, 2022).

119. Defendants had the resources and responsibility to invest in the necessary data security and protection measures. Yet, Defendant 20/20 Eye Care failed to undertake adequate analyses and testing of its own systems and other data security measures to avoid the failures that resulted in the Data Breach.

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

121. Over 41 million patient records were breached in 2019, with a single hacking incident affecting close to 21 million records.[17] Healthcare breaches in 2019 almost tripled those the healthcare industry experienced in 2018, when 15 million patient records were affected by data breach incidents.[18]

122. 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 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.[19] In 2019 that number jumped to 572 incidents, which is likely an underestimate. There continues to be on average at least one health data breach every day.[20]

---

[17] 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, (last visited Mar. 29, 2022).

[18] *Id.*

[19] *Id.*

[20] *Id.*

123. One recent report found that in 2020, healthcare was one of the industries most affected by tracked ransomware incidents.[21]

Defendants' Conduct Violates HIPAA and Industry Standard Data Security Practices.

124. 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 PHI like the data left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

125. The Data Breach resulted from a combination of insufficiencies that indicate Defendants failed to comply with safeguards mandated by HIPAA regulations and industry standards. The security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to adequately catalog the location of Plaintiffs' and Class Members' digital information;

d. Failing to properly encrypt Plaintiffs' and Class Members' PHI;

e. Failing to ensure the confidentiality and integrity of electronic PHI Defendants create, receive, maintain, and transmit in violation of 45 C.F.R. § 164.306(a)(1);

f. 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);

g. 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);

[21] Kat Jerich, *Healthcare hackers demanded an average ransom of $4.6M 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 Mar. 29, 2022).

h. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

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

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

k. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. § 164.306(a)(94);

l. Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq.*;

m. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

n. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

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

126. It is highly probable that the criminal(s) that breached Defendants' systems and acquired Plaintiffs' and Class Members' PII and PHI did so for the purpose of using that data to commit fraud, theft, and other crimes, or for the purpose of selling or providing the PII and PHI to other individuals intending to commit fraud, theft, and other crimes.

127. Given that this is the reason such PII and PHI are sought by criminals, it is similarly probable that Plaintiffs and Class Members have already suffered injury and face a substantial risk for imminent and certainly impending future injury.

128. Defendants acknowledged the risk of fraud, theft, and other crimes faced by victims of the Data Breach in their notices to Plaintiffs and Class Members.

129. 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.[22] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[23]

130. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be understated.[24] "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."[25]

131. More recently, the FTC released an updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding

---

[22] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://www.justice.gov/usao-wdmi/file/764151/download, (last visited Mar. 29, 2022).

[23] *See id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. §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 C.F.R. §603.2(b)

[24] Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, NortonLifeLock (Mar. 13, 2018), https://www.lifelock.com/learn-identity-theft-resources-lasting-effects-of-identity-theft.html, (last visited Mar. 29, 2022).

[25] *Id.* (citing *Identity Theft: The Aftermath 2016*™, Identity Theft Resource Center (2016) https://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf, (last visited Mar. 29, 2022).

network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

132. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect consumers' PII and PHI. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII and PHI as a violation of the FTC Act, 15 U.S.C. § 45.

133. 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.

134. The United States government and privacy experts acknowledge that it may take much time for identity theft to come to light and be detected because identity thieves may wait years before using the stolen data.

135. 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.

Plaintiffs' and Class Members' PII and PHI Are Very Valuable.

136. 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.[26]

137. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[27] 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."[28] The FTC acknowledges that identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[29]

138. 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 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."[30] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives

---

[26] Transcript, *The Information Marketplace: Merging and Exchanging Consumer Data*, FTC (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf, (last visited Mar. 29, 2022).

[27] 17 C.F.R §248.201.

[28] *Id.*

[29] *Guide for Assisting Identity Theft Victims*, FTC (Sep. 2013), https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf, (the "FTC Guide").

[30] 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, (last visited Mar. 29, 2022).

since then indicates that these values—when associated with the loss of PII and PHI to bad actors—would be exponentially higher today.

139. 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.

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

> Keep in mind that a new number probably won't 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) 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 won't 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 shouldn't use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit.[31]

141. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[32] Victims of the Data Breach, including Plaintiffs, will spend, and already have spent, time contacting various agencies, such as the Internal Revenue

[31] SSA, *Identity Theft and Your Social Security Number*, SSA Publ'n No. 05-10064 (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf, (last visited Mar. 29, 2022).

[32] 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.

Service and the SSA. 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.

142. PHI is just as, if not more, valuable than Social Security numbers. According to a report by the FBI's Cyber Division, healthcare records can be sold by criminals for 50 times the price of stolen Social Security numbers or credit card numbers.[33] A file containing private health insurance information can be bought for between $1,200 and $1,300 ***each*** on the black market.[34]

143. PII and PHI are valuable commodities to thieves. PHI 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," commonly referred to as the dark web, for a number of years.[35] As a result of large-scale data breaches, identity thieves and cyber criminals have openly posted stolen Social Security numbers, healthcare information, and other PHI directly on various Internet websites making the information publicly available. These networks and markets consist of hundreds of thousands, if not millions, of nefarious actors who view and access the PHI.

---

[33] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusion*, FBI (Apr. 8, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions/, (last visited Mar. 29, 2022).

[34] 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, (last visited Mar. 29, 2022).

[35] FTC Guide, *supra* n.31.

144. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[36]

145. Professionals tasked with trying to stop fraud and other misuse know that PHI has real monetary value in part because criminals continue their efforts to obtain this data.[37] According to the Identity Theft Resource Center, 2017 saw 1,579 data breaches, representing a 44.7% increase over the record high figures reported a year earlier.[38] The Healthcare sector had the second largest number of breaches among all measured sectors and the highest rate of exposure per breach.[39]

146. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363 according to the Infosec Institute.[40]

147. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

---

[36] *Warning Signs of Identity Theft*, FTC https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft, (last visited Mar. 29, 2022).

[37] George V. Hulme, *Data breaches rise as cybercriminals continue to outwit IT*, CIO MAGAZINE (Sept. 29, 2014), https://www.csoonline.com/article/2688872/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html, (last visited Mar. 29, 2022).

[38] *2017 Annual Data Breach Year-End Review*, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf.

[39] *2018 End -of-Year Data Breach Report*, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/.

[40] *Data Breaches: In the Healthcare Sector*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited Mar. 29, 2022).

148. Legitimate companies also recognize that PII and PHI are valuable assets. 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.

149. Thus, the compromised PII and PHI of Plaintiffs and Class Members have a high value on both legitimate and black markets.

150. 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."[41]

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

152. Immediate notice of a security breach is essential to protect victims such as Plaintiffs and Class Members. Plaintiffs did not receive notice of the Data Breach until four months after the Data Breach was discovered, thus further exacerbating the harm Plaintiffs and Class Members suffered as a result of the Data Breach.

153. Such failure to protect Plaintiffs' and Class Members' PII and PHI, and the delay in their notification 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

[41] *See* FBI, *supra* n.35.

data points stolen are persistent—for example, names, dates of birth, Social Security numbers, and prescription medication data—as opposed to transitory, criminals who access, steal, 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.

154. 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.

155. 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.

156. Despite Defendants' failure to protect Plaintiffs' and Class Members' PII and PHI, they have only offered to provide them with trivial compensation or an inadequate remedy, such as free credit monitoring or identity protection services. Upon information and belief, Plaintiffs and Class Members also were not offered or provided any adequate compensation or remedy to protect their information taken in this Data Breach.

Plaintiffs and Class Members Suffered Long-Lasting Damages.

157. The ramifications of Defendants' failure to keep Plaintiffs' and Class Members' PII and PHI secure are long lasting and severe. Once PII and PHI are stolen, fraudulent use of that information and damage to victims may continue for years.

158. Fraudulent activity might not show up for prolonged periods of time—potentially years after the PII and PHI are divulged to unauthorized third parties. Criminals often trade stolen PII and PHI on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PHI on the internet, thereby making such information publicly available. These cybercriminals and other unauthorized third parties are now free to exploit and misuse that PII and PHI without any ability for Plaintiffs and Class Members to recapture and erase the PII and PHI from further dissemination. Plaintiffs' and Class Members' PII and PHI is forever compromised, and this PII and PHI were unique to the information that Defendants inadequately and improperly safeguarded.

159. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[42] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[43]

160. Healthcare related data is among the most sensitive and personally consequential when compromised. A report focusing on health-care breaches found that the "average total cost to resolve an identity theft-related incident…came to about $20,000."[44] Further, a majority of the

---

[42] *See* Donna Parent, *Medical ID Theft Checklist*, IDENTITYFORCE (May 18, 2019), https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[43] *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches*, EXPERIAN (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[44] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010) https://www.cnet.com/tech/services-and-software/study-medical-identity-theft-is-costly-for-victims/.

victims were forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage. Moreover, almost 50% of the victims lost their health care coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.[45]

161. As the FTC recognizes, identity thieves can use this PHI to commit an array of crimes including identity theft, and medical and financial fraud.

162. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[46]

163. Here, not only was sensitive medical information divulged and compromised, but also patient Social Security numbers were involved. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even

---

[45] *Id.*

[46] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," KAISER HEALTH NEWS, (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

years, later.[47] This time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

164. 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. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

165. Moreover, according to Robert P. Chappell, Jr., a law enforcement professional, a minor's information can be stolen and used until the minor turns eighteen years old before the minor even realizes he or she has been victimized.[48]

166. The risk to Class Members who are children is substantial given their age and lack of established credit because their information can be used to create a "clean identity slate." It is not surprising then that one report found that children are 51% more likely be victims of identity theft than adults.[49] Cybercriminals on the Dark Web have been caught selling Social Security numbers of infants for $300 per number to be used on fraudulent tax returns.[50]

---

[47] *Identity Theft and Your Social Security Number*, SSA (June 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf, (last visited Mar. 29, 2022).

[48] Brett Singer, *What is Child Identify Theft?*, Parents, https://www.parents.com/kids/safety/tips/what-is-child-identity-theft/ (last visited July 28, 2021).

[49] Avery Wolfe, *How Data Breaches Affect Children*, Axion Cyber Sols. (Mar. 15, 2018), https://axiomcyber.com/data-breach/how-data-breaches-affect-children/, (last visited Mar. 29, 2022).

[50] *Id.*

167. The PII and PHI belonging to Plaintiffs and Class Members is private and sensitive in nature and was left inadequately protected by Defendants who did not obtain Plaintiffs' or Class Members' consent to disclose their PII and PHI to any other person as required by applicable law and industry standards. The Data Breach was a direct and proximate result of Defendants' failure to: (a) properly safeguard and protect Plaintiffs' and Class Members' PII and PHI from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII and PHI; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

168. Had Defendant 20/20 Eye Care remedied the deficiencies in its data security system and adopted security measures and protocols recommended by experts in the field, and had Defendant iCare not been negligent, Defendants would have prevented the intrusion and, ultimately, the theft of Plaintiffs' and Class Members' PII and PHI.

169. As a direct and proximate result of Defendants' wrongful actions and inaction, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that

"[r]esolving the problems caused by identity theft [could] take more than a year for some victims."[51]

170. As a result of the Defendants' failure to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII and PHI;

b. Unauthorized use and misuse of their PII and PHI;

c. The loss of the opportunity to control how their PII and PHI are used;

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

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from 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 and fraud;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

g. The continued risk to their PII and PHI that is subject to further breaches so long as Defendants fails to undertake appropriate measures to protect the PII and PHI in 20/20's possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

171. In addition to a remedy for the economic harm, Plaintiffs and the Class maintain an undeniable and continuing interest in ensuring that their PII and PHI that remains in the possession of Defendants is secure, remains secure, and is not subject to further theft.

---

[51] Erika Harrell, Ph.D. and Lynn Langton, Ph.D., *Victims of Identity Theft, 2012*, DOJ, Off. of Just. Programs, Bureau of Just. Statistics (Dec. 2013), https://www.bjs.gov/content/pub/pdf/vit12.pdf, (last visited Mar. 29, 2022).

CLASS ACTION ALLEGATIONS

172. Pursuant to the provisions of Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and 23(c)(5), Plaintiffs seek to bring this class action on behalf of themselves and a nationwide class (the "Nationwide Class") defined as follows:

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

173. The Nationwide Class asserts claims against Defendant 20/20 Eye Care for negligence, negligent supervision, and injunctive relief under the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§ 501.201, *et. seq.*, and against Defendant iCare for negligence and injunctive relief under FDUTPA.

174. Alternatively, 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 accessed and divulged by the Data Breach.**

175. The Florida Subclass asserts claims against Defendant 20/20 Eye Care for negligence, negligent supervision, and injunctive relief under the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§ 501.201, *et. seq.*, and against Defendant iCare for negligence and injunctive relief under FDUTPA.

176. Where appropriate, the Nationwide Class and the Florida Subclass are collectively referred to as the "Class."

177. 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.

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

179. 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.

180. 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.

181. ***Numerosity***. Consistent with Fed. R. Civ. P. 23(a)(1), the Nationwide Class and the Florida Subclass are so numerous that joinder of all members is impracticable. While the exact number of Nationwide Class Members is unknown, upon information and belief, it is in excess of three million, and the Florida Subclass likely contains a large percentage of Class Members.

182. ***Commonality and Predominance***. Consistent with Fed. R. Civ. P. 23(a)(2) and (b)(3), this action involves common questions of law and fact that predominate over any questions that may affect only individual Class Members. Such common questions include:

a. whether Defendants engaged in the wrongful conduct alleged in this Consolidated Complaint;

b. whether Defendants' conduct was unfair, unconscionable, and/or unlawful;

c. whether Defendants failed to implement and maintain adequate and reasonable systems and security procedures and practices to protect Plaintiffs' and Class Members' PII and PHI;

d. whether Defendants owed a duty to Plaintiffs and Class Members to adequately protect their PII and PHI and to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

e. whether Defendants breached their duties to protect the PII and PHI of Plaintiffs and Class Members by failing to provide adequate data security

and failing to provide appropriate and adequate notice of the Data Breach to Plaintiffs and Class Members;

f. whether Defendants' conduct was negligent;

g. whether Defendant 20/20 Eye Care's conduct constituted negligent supervision;

h. whether Defendants knew or should have known that their computer systems were vulnerable to being compromised;

i. 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 Plaintiffs' and Class Members' PII and PHI;

j. 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 Plaintiffs' and Class Members' PII and PHI;

k. whether Plaintiffs and Class Members suffered injury, including ascertainable losses, as a result of Defendants' conduct (or failure to act);

l. whether Plaintiffs and Class Members are entitled to recover damages; and

m. whether Plaintiffs and Class Members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

183. ***Typicality***. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of the claims of other Class Members in that Plaintiffs, like all Class Members, had their PII and PHI compromised, breached, and stolen in the Data Breach. Plaintiffs and all Class Members were injured through the misconduct of Defendants, described in this Second Amended Consolidated Complaint, and assert the same claims for relief.

184. ***Adequacy***. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs and counsel will fairly and adequately protect the interests of the Class. Plaintiffs are members of the Class they seek to represent; are committed to pursuing this matter against Defendants to obtain relief for the Class; and have no interests that are antagonistic to, or in conflict with, the interests of other Class Members. Plaintiffs retained counsel who are competent and experienced in litigating class actions

and complex litigation, including privacy litigation of this kind. Plaintiffs and their counsel intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

185. ***Superiority***. Consistent with Fed. R. Civ. P. 23(b)(3), 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.

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

187. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(1), 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 their 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.

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

189. 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 Defendants owed a legal duty to Plaintiffs and the Class Members;

c. whether Defendants failed to take adequate and reasonable steps to safeguard the PII and PHI of Plaintiffs and Class Members;

d. whether Defendants failed to adequately monitor their data security systems;

e. whether Defendants failed to comply with applicable laws, regulations, and industry standards relating to data security;

f. whether Defendants knew or should have known that they did not employ adequate and reasonable measures to keep Plaintiffs' and Class members' PII and PHI secure;

g. 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; and

h. whether Defendant 20/20 Eye Care negligently supervised its employee(s).

COUNT I

Negligence

As to Defendant 20/20 Eye Care

On Behalf of Plaintiffs and the Nationwide Class, or alternatively the Florida Subclass

190. Plaintiffs incorporate paragraphs 1-171 of the Second Amended Consolidated Complaint as if fully set forth herein.

191. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

192. Defendant 20/20 Eye Care collected, stored, used, and benefited from the non-public PII and PHI of Plaintiffs and Class Members in the procurement and provision of medical service benefits for Plaintiffs and Class Members.

193. Defendant 20/20 Eye Care had full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and Class Members could and would suffer if the PII and PHI were wrongfully disclosed.

194. By collecting, storing, and using Plaintiffs' and Class Members' PII and PHI, Defendant 20/20 Eye Care owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII and PHI. Defendant 20/20 Eye Care owed a duty to prevent the PII and PHI they received from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

195. Defendant 20/20 Eye Care was required to prevent foreseeable harm to Plaintiffs

and Class Members, and they therefore had a duty to take adequate and reasonable steps to safeguard their sensitive PII and PHI from unauthorized release or theft. This duty included: (1) designing, maintaining, and testing its data security systems, data storage architecture, and data security protocols to ensure Plaintiffs' and Class Members' PII and PHI in its possession was adequately secured and protected; (2) implementing processes that would detect an unauthorized breach of its security systems and data storage architecture in a timely and adequate manner; (3) timely acting on all warnings and alerts, including public information, regarding its security vulnerabilities and potential compromise of the PII and PHI of Plaintiffs and Class Members; and (4) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements.

196. Defendant 20/20 Eye Care 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 security practices of Defendant in its collection, storage, and use 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 malicious actors routinely attempt to steal such information for use in nefarious purposes, but Defendant also knew that it was more likely than not Plaintiffs and Class Members would be harmed as a result.

197. Defendant 20/20 Eye Care's duties to use adequate and reasonable security measures also arose as a result of the special relationship that existed between it, on the one hand, and Plaintiffs and Class Members, on the other hand. This special relationship arose because Defendant collected, stored, and used the PII and PHI of Plaintiffs and Class Members for the procurement and provision of health services for Plaintiffs and Class Members. Defendant alone

could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

198. Additionally, the policy of preventing future harm weighs in favor of finding a special relationship between Defendant 20/20 Eye Care and Plaintiffs and Class Members. If companies are not held accountable for failing to take adequate and 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.

199. Defendant 20/20 Eye Care also owed a duty to timely disclose the material fact that its computer systems and data security practices and protocols were inadequate to safeguard users' personal, health, and financial data from theft.

200. The injuries suffered by Plaintiffs and Class Members were proximately and directly caused by Defendant 20/20 Eye Care's failure to follow reasonable, industry standard security measures to protect Plaintiffs' and Class Members' PII and PHI.

201. 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.

202. If Defendant 20/20 Eye Care had implemented the requisite, industry standard security measures and exercised adequate and reasonable care, data thieves would not have been able to take the PII and PHI of Plaintiffs and Class Members.

203. Defendant 20/20 Eye Care breached these duties through the conduct alleged here in this Second Amended Consolidated Complaint by, including without limitation, failing to protect the PII and PHI in their possession; failing to maintain adequate computer systems and

allowing unauthorized access to and exfiltration of 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 its 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.

204. But for Defendant 20/20 Eye Care's 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 Defendant 20/20 Eye Care's failure to exercise adequate and reasonable care and use commercially adequate and reasonable security measures, the PII and PHI of Plaintiffs and Class Members were accessed by ill-intentioned individuals 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.

205. There is a temporal and close causal connection between Defendant 20/20 Eye Care's failure to implement security measures to protect the PII and PHI of current and former patients and the harm suffered, or risk of imminent harm suffered, by Plaintiffs and Class Members.

206. It was foreseeable that Defendant 20/20 Eye Care's failure to exercise reasonable care to safeguard the PII and PHI in its 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.

207. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant 20/20 Eye Care knew of or should have

known of the inherent risks in collecting and storing PII and PHI, the critical importance of providing adequate security of PII and PHI, the current cyber scams being perpetrated on PII and PHI, and that it had inadequate protocols, including security protocols in place to secure the PII and PHI of Plaintiffs and Class Members.

208. Defendant 20/20 Eye Care's own conduct created the foreseeable risk of harm to Plaintiffs and Class Members. Defendant 20/20 Eye Care's misconduct included their failure to take the steps and opportunities to prevent the Data Breach and their failure to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII and PHI of Plaintiffs and Class Members.

209. Plaintiffs and Class Members have no ability to protect their PII and PHI that was and is in Defendant's possession. Defendant 20/20 Eye Care alone was and is in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

210. As a direct and proximate result of Defendant 20/20 Eye Care's negligence as alleged above, Plaintiffs and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII and PHI;

b. Unauthorized use and misuse of their PII and PHI;

c. The loss of the opportunity to control how their PII and PHI are used;

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

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from 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 and fraud;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

g. The continued risk to their PII and PHI that is subject to further breaches so long as Defendants fails to undertake appropriate measures to protect the PII and PHI in 20/20's possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

212. 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 and PHI. 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.

213. Defendant 20/20 Eye Care solicited, gathered, and stored PII and PHI of Plaintiffs and Class Members to facilitate transactions which affect commerce.

214. Defendant 20/20 Eye Care violated the FTC Act (and similar state statutes) and HIPAA, 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.

215. Defendant 20/20 Eye Care violations of the FTC Act (and similar state statutes) and HIPAA are evidence of negligence.

216. Plaintiffs and Class Members are within the class of persons that the FTC Act (and similar state statutes) and HIPAA were intended to protect.

217. The harm that occurred as a result of the Data Breach is the type of harm the FTC

Act (and similar state statutes) and HIPAA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ adequate and reasonable data security measures caused the same harm as that suffered by Plaintiffs and Class Members.

218. As a direct and proximate result of Defendant 20/20 Eye Care's violations of the above-mentioned statutes (and similar state statutes), 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.

COUNT II

Negligent Supervision

As to Defendant 20/20 Eye Care

On Behalf of Plaintiffs and the Nationwide Class, or alternatively the Florida Subclass

219. Plaintiffs incorporate paragraphs 1-171 of the Second Amended Consolidated Complaint as if fully set forth herein.

220. As previously alleged, Defendant 20/20 Eye Care collected, stored, used, and benefited from the non-public PII and PHI of Plaintiffs and Class Members in the procurement and provision of medical service benefits for Plaintiffs and Class Members.

221. Additionally, Defendant 20/20 Eye Care had full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and Class Members could and would suffer if the PII and PHI were wrongfully disclosed. Defendant 20/20 Eye Care also had the ability to adequately supervise and knew it was necessary to supervise and control its employees to prevent them from intentionally harming Plaintiffs and Class Members by mishandling and improperly disclosing Plaintiffs and Class Members' PII and PHI.

222. At all times relevant hereto, Defendant 20/20 Eye Care's employees were acting in

the normal course and scope of their employment.

223. Defendant 20/20 Eye Care owed a duty to Plaintiffs and Class Members to supervise its employees to ensure its employees recognized the duties owed to patients—including Plaintiffs and Class Members—to protect and safeguard the non-public PII and PHI collected, stored, and used by Defendant 20/20 in the procurement and provision of services.

224. Defendant 20/20 Eye Care breached its duty to Plaintiffs and Class Members by failing to (a) exercise reasonable care in the supervision its employees entrusted with access to and security of Plaintiffs' and Class Members' PII and PHI, (b) exercise appropriate care supervising employees on cyber security measures regarding the safety of patient information; (c) exercise reasonable care supervising employee reviews of security practices and procedures, (d) exercise reasonable care supervising its employees' access controls to Plaintiffs' and Class Members' PII and PHI—including the ability to access, read, edit, use, and delete data, (e) exercise reasonable care in the supervision of its employees regarding the implementation, upgrading, and use of adequate password and authentication methods to restrict access to and protect Plaintiffs' and Class Members' PII and PHI, and (f) supervise by way of monitoring employee activities relating to removing and/or deleting of patient data—specifically Plaintiffs' and Class Members' PII and PHI and preventing such actions.

225. As a result of these breaches, unauthorized access to Plaintiffs' and Class Members' PII and PHI was allowed, resulting in the Data Breach.

226. Defendant 20/20 Eye Care knew or should have known about the fitness—or lack thereof—of its employees, and whether employees with access and ability to delete Plaintiffs' and Class Members PII and PHI required additional supervision.

227. Defendant 20/20 Eye Care negligently supervised its employees by it failing to take

appropriate action regarding the lack of fitness of one or more employees with access and ability to delete Plaintiffs' and Class Members PII and PHI. As a result, unauthorized use of Plaintiffs' and the Class Members' PII and PHI was allowed, resulting in the Data Breach.

228. The injuries suffered by Plaintiffs and Class Members were proximately and directly caused by Defendant 20/20 Eye Care's failure to exercise its duty to adequately and reasonably supervise its employees.

229. As a direct and proximate result of Defendant 20/20 Eye Care's negligent supervision, Plaintiffs and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII and PHI;

b. Unauthorized use and misuse of their PII and PHI;

c. The loss of the opportunity to control how their PII and PHI are used;

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

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from 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 and fraud;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

g. The continued risk to their PII and PHI that is subject to further breaches so long as Defendant 20/20 Eye Care fails to undertake appropriate supervisory measures to protect the PII and PHI in its possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

COUNT III

Negligence

As to Defendant iCare

On Behalf of Plaintiffs and the Nationwide Class, or alternatively the Florida Subclass

230. Plaintiffs incorporate paragraphs 1-171 of the Second Amended Consolidated Complaint as if fully set forth herein.

231. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

232. As alleged above, Defendant 20/20 Eye Care collected, stored, used, and benefited from the non-public PII and PHI of Plaintiffs and Class Members in the procurement and provision of medical service benefits for Plaintiffs and Class Members.

233. Defendant 20/20 Eye Care had full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and Class Members could and would suffer if the PII and PHI were wrongfully disclosed.

234. By acquiring 20/20 Eye Care, a company that collects, stores, and uses PII and PHI, and by taking over management and operation of 20/20 Eye Care, Defendant iCare owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII and PHI, including a duty to prevent the PII and PHI from being compromised, lost, stolen, accessed, and misused by unauthorized persons. This duty included, among other things: (1) exercising reasonable care in the its management and oversight of its acquired company (20/20 Eye Care), integrating and implementing appropriate security mechanisms to insure that security and best practices were provided to protect Plaintiffs' and Class Members' PII and PHI, and on cyber security measures regarding the safety of patient information; (2) exercising reasonable care in the acquisition of 20/20 Eye Care and all activities associated with that acquisition; (3) exercising reasonable care in dealing with access to sensitive information

after the acquisition of 20/20 Eye Care; and (4) ensuring that no persons had unnecessary or unreasonable access to Plaintiffs' and Class Members' PII and PHI.

235. Defendant iCare breached these duties. It failed to exercise reasonable care in the management of those entrusted with access to Plaintiffs' and Class Members' PII and PHI, failed to exercise appropriate care on cyber security measures regarding the safety of patient information; failed to exercise reasonable care in the acquisition of 20/20 Eye Care and the activities associated with that acquisition; and failed to ensure that no persons had more access than necessary or appropriate, to Plaintiffs' and Class Members' PII and PHI.

236. As a result of these breaches, and in combination with the negligence of 20/20 Eye Care as alleged above, unauthorized use of Plaintiffs' and the Class members' PII and PHI was allowed, resulting in the Data Breach.

237. The injuries suffered by Plaintiffs and Class Members were proximately and directly caused by Defendant iCare's failure to exercise adequate and reasonable care in the above and failure to properly and safely handle the transition of ownership of 20/20 Eye Care.

238. As a direct and proximate result of Defendant 20/20 Eye Care's negligence as alleged above, Plaintiffs and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII and PHI;

b. Unauthorized use and misuse of their PII and PHI;

c. The loss of the opportunity to control how their PII and PHI are used;

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

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from 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 and fraud;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

g. The continued risk to their PII and PHI that is subject to further breaches so long as Defendants fails to undertake appropriate measures to protect the PII and PHI in 20/20's possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

COUNT IV

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

As to all Defendants

On Behalf of Plaintiffs and the Nationwide Class, or alternatively the Florida Subclass

239. Plaintiffs incorporate paragraphs 1-171 of the Second Amended Consolidated Complaint as if fully set forth herein.

240. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class; in the alternative, Plaintiffs bring this claim on behalf of themselves and the Florida Subclass.

241. This cause of action is brought pursuant the FDUTPA, which, pursuant to Fla. Stat. § 501.202, requires such claims be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

242. Defendants' offer, provision, and sale or services at issue in this case are "consumer transaction[s]" within the scope of the FDUTPA. *See* Fla. Stat. §§ 501.201-501.213.

243. Plaintiffs and the Class Members, as "individual[s]," are "consumer[s]" as defined by the FDUTPA. *See* Fla. Stat. § 501.203(7).

244. Defendants helped manage health insurance benefits on Plaintiffs' and the Class Members' behalf.

245. Defendants offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. § 501.203.

246. Plaintiffs and the Class Members paid for or otherwise availed themselves and received services from Defendants, primarily for personal, family, or household purposes.

247. Defendants engaged in the conduct alleged in this Second Amended Consolidated Class Action Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of health-related benefits to or for Plaintiffs and Class Members.

248. Defendants' acts, practices, and omissions were done in the course of Defendants' business of offering, providing, and selling health-related benefits throughout Florida and the United States.

249. The unfair, unconscionable, and unlawful acts and practices of Defendants alleged herein, and in particular the decisions regarding data security, emanated and arose within the state of Florida, within the scope of the FDUTPA.

250. Defendants, headquartered and operating in and out of Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. failure to implement and maintain reasonable and adequate computer systems and data security practices to safeguard patient PII and PHI;

b. omitting, suppressing, and concealing the material fact that their computer systems and data security practices were inadequate to safeguard patient PII and PHI from theft;

c. failure to protect the privacy and confidentiality of Plaintiffs' and Class Members' PII and PHI;

d. continued acceptance and storage of patient PII and PHI after Defendants knew or should have known of the security vulnerabilities that were exploited in the Data Breach;

e. continued acceptance and storage of patient PII and PHI after Defendants knew or should have known of the Data Breach and before it allegedly remediated the Data Breach.

251. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including by not limited to the FTC Act, 15 U.S.C. § 41, *et seq.*, and the FDUTPA, Fla. Stat. § 501.171(2).

252. Defendants knew or should have known that the 20/20 Eye Care's computer system and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and PHI and that the risk of a data breach or theft was high.

253. Plaintiffs have standing to pursue this claim because as a direct and proximate result of Defendants' violations of the FDUTPA, Plaintiffs and Class Members have been "aggrieved" by a violation of the FDUTPA and bring this action to obtain a declaratory judgment that Defendants' acts or practices violate the FDUTPA. *See* Fla. Stat. § 501.211(a).

254. Plaintiffs also have standing to pursue this claim because, as a direct result of Defendants' knowing violation of the FDUTPA, Plaintiffs are at a substantial and imminent risk

of future identity theft. Defendants still possess Plaintiffs' and the Class Members PII and PHI, and some Plaintiffs' PII and PHI has been both accessed and misused by unauthorized third parties, which is evidence of a substantial and imminent risk of future identity theft for all Plaintiffs and Class Members.

255. Plaintiffs and Class Members are entitled to injunctive relief to protect them from the substantial and imminent risk of future identity theft, 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 20/20 Eye Care's systems on a periodic basis, and ordering prompt correction of 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 security personnel regarding any new or modified procedures;

d. ordering that Defendants segment patient data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

e. ordering that Defendants purge, delete, and destroy patient PII and PHI not necessary for its provisions of services in a reasonably secure manner;

f. ordering that Defendants conduct regular database scans and security 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; and

h. ordering Defendants to meaningfully educate patients about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps patients should take to protect themselves.

256. Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow patient-consumers to make informed purchasing decisions and to protect Plaintiffs, Class Members and the public from Defendant's unfair methods of competition and unfair, unconscionable, and unlawful practices. Defendants' wrongful conduct as alleged in this Second Amended Consolidated Class Action Complaint has had widespread impact on the public at large.

257. The above unfair, unconscionable, and unlawful practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to patient-consumers or to competition.

258. Defendants' actions and inactions in engaging in the unfair, unconscionable, and unlawful practices and described herein were negligent, knowing and willful, and/or wanton and reckless.

259. Plaintiffs and Class Members seek relief under the FDUTPA, Fla. Stat. §§ 501.201, *et seq.*, including, but not limited to, a declaratory judgment that Defendants' actions and/or practices violate the FDUTPA; injunctive relief enjoining Defendants, their employees, parents,

subsidiaries, affiliates, executives, and agents from violating the FDUTPA, 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 20/20's systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors, ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring, ordering that Defendants audit, test, and train security personnel regarding any new or modified procedures, ordering that Defendants segment patient data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system, ordering that Defendants purge, delete, and destroy patient PII and PHI not necessary for its provisions of services in a reasonably secure manner, ordering that Defendants conduct regular database scans and security checks, 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, ordering Defendants to meaningfully educate patients about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps patients should take to protect themselves, and any other just and proper relief.

RELIEF REQUESTED

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Class, respectfully request the following relief:

a. An order certifying this case as a class action on behalf of the Class, defined above, appointing Plaintiffs as Class representatives and appointing the undersigned counsel as Class counsel;

b. A mandatory permanent injunction directing Defendants to adequately safeguard

Plaintiffs' and the Class' PII and PHI by implementing improved security procedures and measures as outlined above;

c. An award of other injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

d. An award of restitution and compensatory, consequential, and general damages to Plaintiffs and Class Members, including nominal damages as allowed by law in an amount to be determined at trial or by this Court;

e. An award of actual damages to Plaintiffs and Class Members in an amount to be determined at trial or by this Court;

f. An award of reasonable litigation expenses and costs and attorneys' fees to the extent allowed by law;

g. An award to Plaintiffs and Class Members of pre- and post-judgment interest, to the extent allowable; and

h. 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.

Dated: March 29, 2022

Respectfully submitted,

/s/ Francesca Kester

JEAN S. MARTIN *(pro hac vice)*
RYAN J. MCGEE, Florida Bar No. 64957
FRANCESCA KESTER, Florida Bar No. 1021991
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel: 813/223-5505

Jmartin@forthepeople.com
rmcgee@forthepeople.com
fkester@forthepeople.com

Chair of Plaintiffs' Executive Committee

ROBBINS GELLER RUDMAN & DOWD LLP
DOROTHY P. ANTULLIS (0890421)
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Phone: 561/750-3000
Fax: 561/750-3364
dantullis@rgrdlaw.com

Liaison Counsel for Plaintiffs

CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
GAYLE M. BLATT (*pro hac vice*)
110 Laurel Street
San Diego, CA 92101
Telephone: 619/238-1811
gmb@cglaw.com

Plaintiffs' Interim Co-Lead Class Counsel

CHESTNUT CAMBRONNE PA
BRYAN L. BLEICHNER (*pro hac vice*)
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: 612/339-7300
612/336-2940 (fax)
bbleichner@chestnutcambronne.com

Plaintiffs' Interim Co-Lead Class Counsel

MARKOVITS, STOCK & DEMARCO, LLC
TERENCE R. COATES *(pro hac vice)*
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Telephone: 513/651-3700
513/665-0219 (fax)
tcoates@msdlegal.com

Plaintiffs' Executive Committee Member

THE LYON FIRM
JOSEPH M. LYON (*pro hac vice*)
2754 Erie Avenue
Cincinnati, OH 45208
Telephone: 513/381-2333
513/721-1178 (fax)
jlyon@thelyonfirm.com

Plaintiffs' Executive Committee Member

CLAYEO C. ARNOLD
A PROFESSIONAL LAW CORP.
M. ANDERSON BERRY (*pro hac vice*)
865 Howe Avenue
Sacramento, CA 95825
Telephone: 916/239-4778
aberry@justice4you.com

Plaintiffs' Executive Committee Member

HELLMUTH & JOHNSON PLLC
NATHAN D. PROSSER (*pro hac vice*)
8050 West 78th Street
Edina, MN 55439
Telephone: 952/941-4005
nprosser@hjlawfirm.com

Plaintiffs' Executive Committee Member

MASON LLP
GARY MASON (*pro hac vice*)
5101 Wisconsin Avenue, NW, Suite 305
Washington, D.C. 20016
Telephone: 202/429-2290
gmason@masonllp.com

CERTIFICATE OF SERVICE

I hereby certify that on March 29, 2022, I electronically filed the foregoing document with the Clerk of Court using CM/ECF. I also certify that the foregoing document is being served this day on all counsel of record or pro se parties in the manner specified, either via transmission of Notices of Electronic Filing generated by CM/ECF or in some other authorized manner for those counsel or parties who are not authorized to receive electronically Notices of Electronic Filing.

/s/ Francesca Kester
FRANCESCA KESTER, Florida Bar No. 1021991