UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

Kristi Hoffman-Mock, individually and on behalf of all others similarly situated, Plaintiff, v. 20/20 EYE CARE NETWORK, INC., and ICARE HEALTH SOLUTIONS, LLC, Defendants.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Kristi Hoffman-Mock ("Plaintiff") brings this Class Action Complaint against Defendants 20/20 Eye Care Network, Inc. ("20/20") and iCare Health Solutions, Inc. ("iCare" and collectively, "Defendants") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. Plaintiff brings this class action to provide relief to 3.2 million similarly situated people harmed by Defendants failure to secure personally identifiable information ("PII") and private health information ("PHI").

2. Defendant 20/20 is an entity that provides eye and hearing care services and administration.

3. Upon information and belief, Defendant iCare partially owns and is a partner with 20/20 to provide integrated eye health, hearing health, and administrative services in Florida.

4. In May 2021, Plaintiff received a letter dated May 28, 2021 that stated in January 2021, PII/PHI that was on 20/20's systems had been viewed, seen, or accessed by unauthorized

Devine Goodman & Rasco, LLP 2800 Ponce De Leon Boulevard, Suite 1400, Coral Gables, Florida 33134 P 305.374.8200 F 305.374.8208

third parties (the "Data Breach"). The notifications revealed that hackers gained unauthorized access to 20/20's system and deleted files.

5. This Data Breach occurred because Defendants failed to implement reasonably adequate cyber-security measures to protect Plaintiff's PII/PHI. The deficiencies in Defendants cyber-security measures allowed the hackers to access patient data, which included the ability to view and edit the data.

6. Defendants disregarded the rights of Plaintiff and putative Class Members by:

a. Intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected;

b. Failing to disclose to their patients the material fact that they did not have adequate computer systems and security practices to safeguard their PII/PHI;

c. Failing to take available steps to prevent the Data Breach; and

d. Failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

7. Because of Defendants' failure to secure Plaintiff's and Class Members' PII/PHI, hackers have stolen their PII/PHI. As such, Plaintiff and Class Members, which includes minors, face a substantial increased risk of identity theft. Further, Plaintiff and Class Members have paid, or will have to pay, private monitoring companies to protect themselves. On top of paying for monitoring, Plaintiff had fraudulent charges on her credit card (discussed below). This makes clear that the Data Breach will put Plaintiff and Class Members at a heightened risk for theft and fraud for the rest of their lives.

8. Plaintiff seeks, among other things, that the Defendants be required to disclose the nature of the information taken by hackers. Further, Defendants must adopt sufficient cyber-security measures to prevent incidents like this Data Breach from happening in the future.

9. On behalf of all others similarly situated, Plaintiff alleges claims for negligence, invasion of privacy, breach of implied contract, unjust enrichment, breach of fiduciary duty, breach

Devine Goodman & Rasco, LLP 2800 Ponce De Leon Boulevard, Suite 1400, Coral Gables, Florida 33134 P 305.374.8200 F 305.374.8208

of confidence and violation of Florida's Deceptive and Unfair Trade Practices Act.

II. PARTIES

10. Plaintiff Kristi Hoffman-Mock is a citizen of Florida residing in Summerfield, Florida.

11. Defendant 20/20 Eye Care Network, Inc. is a vision care company that offers third party administrative services. 20/20 contracts with optometrists, ophthalmologists, ambulatory surgical centers, and retail vision centers to provide a full spectrum of eye care needs. Its management services include claims processing, credentialing, management utilization, and network leasing.

12. Defendant 20/20 owns 20/20 Hearing Care Network, Inc., which is a health care provider for audiology and related administrative work.

13. Defendant iCare Health Solutions, LLC is an integrated specialty network and administrator of comprehensive ocular care services. It contracts with health plans and multispecialty clinics to deliver comprehensive ocular health solutions through a network of optometrists and ophthalmologists.

14. In September of 2020, Defendant iCare, backed by private equity firm Pine Tree Equity IV, LP, invested in Defendant 20/20. iCare now controls 20/20 in whole or in part, which makes it the largest ophthalmology and optometry provider with over 55 locations and the largest managed service provider.

III. JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act. (28 U.S.C. § 1332(d)(2)) The amount in controversy exceeds $5 million, exclusive of costs and interest. There are in excess of 100 putative class members, at least some of whom have a different citizenship from Defendants.

16. This Court has personal jurisdiction over Defendant because Defendant iCare Health Solutions, LLC has its principal place of business within this District at 7352 NW 34 Street Miami, Florida 33122.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. The compromised 20/20 network that hackers stole Plaintiffs' PII/PHI is within the district. Further, 20/20 is based in the District and likely stores more PII/PHI in the district.

IV. FACTUAL ALLEGATIONS

A. Background of the Data Breach

18. Plaintiff received medical services from 20/20 Eye Care Network, Inc. and 20/20 Hearing Care Network, Inc.

19. Defendants reported to the Maine Attorney General that the Data Breach affected nearly 3.3 million individuals.[1] The Defendants reported the breach as "insider wrongdoing" according to the Maine Attorney General's data breach notification. Further, Defendants discovered the breach on February 18, 2021 and the breach occurred on January 11, 2021.

20. However, it was not until May 28, 2021 that Plaintiff received a letter informing her of the breach. The letter explained that the 20/20 Hearing Care Network helps manage her benefits and that Plaintiff's PII/PHI was exposed.

21. Defendants' letters stated that the information that was exposed in the data breach may have included:

- Name
- Date of birth
- Social Security Number
- Member identification number
- Health insurance information

22. Defendants acquire a large number of patients' PHI and PII on a regular basis and maintain this data. Defendants require customers/patients to provide this information through the

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/946029d6-7945-4a23-89c1-0ea29e9c18a2.shtml (last visited Jul. 7, 2021).

ordinary course of business so that they can process claims submitted by patient providers.

23. According to the Notice of Data Breach letters and letters sent to state Attorneys General, the PHI and PII that Defendants collect "was accessed or downloaded prior to deletion."[2]

B. Defendants Were Aware of the Risks of a Data Breach

24. Defendants knew that there was a risk of data breaches in the healthcare industry.

25. Data breaches have become widespread. For example, The American Medical Association ("AMA") has warned that 83% of physicians have experienced some form of cyberattack and 1-in-2 physicians are "very" or "extremely" concerned about future cyberattacks.

26. Indeed, data breaches, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") has issued a warning to potential targets, so they are aware of, and prepared for, potential attacks. The FBI says, "malicious actors target healthcare related systems, perhaps for the purpose of obtaining [PHI and PII]".[3] Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and foreseeable to the public and to anyone in Defendants' industry, including Defendants.

C. Personally Identifiable Information

27. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[4] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[5]

---

[2] https://2020incident.com/home.htm (last visited July 7, 2021).

[3] 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 accessed July 7, 2021)

[4] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited July 7, 2021).

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

28. Hackers targeted and stole the PII/PHI of Plaintiff and Class members to engage in identity theft and or to sell it to other criminals who will purchase the PII/PHI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

29. Plaintiff and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. They are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

D. Defendants Fail to Comply with HIPAA and Industry Standard Practices

30. Title II of HIPAA authorizes the Department of Health and Human Services ("HHS") to create rules to standardize the handling of PHI. 42 U.S.C. §§ 1301, *et seq*. The Data Breach resulted from a combination of insufficiencies that indicate that the Defendants failed to comply with the standards created by the HHS.

31. The failures to comply with these standards include:

a. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants create, receive, maintain, and transmit in violation of 45 CFR 164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

c. Failing to implement policies and procedure to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

d. 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 CFR 164.308(a)(6)(ii);

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

f. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the

alien registration number, government passport number, employer or taxpayer identification number." *Id*.

privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules in their workforce in violation of 45 CFR 164.306(a)(94);

h. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, et seq.;

i. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45 CFR 164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

32. Defendants were at all times fully aware of their obligation to protect the PII/PHI of customers/patients and prospective customers/patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

E. The Value of PII to Cyber Criminals

33. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. Information such as dates of birth and Social Security numbers, however, are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

34. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6]

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

35. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[7]

36. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

37. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[8]

38. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit

---

[7] SSA, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 7, 2021).

[8] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 7, 2021).

> record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[9]

39. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all essential PII and PHI to mimic the identity of the user. The personal data of Plaintiff and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and members of the Class represents essentially one-stop shopping for identity thieves.

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

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

42. PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII or PHI on a number of Internet websites.

---

[9] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 7, 2021).

[10] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29 (last visited July 7, 2021).

The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

43. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

44. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. For example, criminals can use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendants' former and current patients whose Social Security numbers have been compromised 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.

45. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver's license number or government-issued identification number, name, and date of birth.

46. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[11]

47. Among other forms of fraud, identity thieves may obtain driver's licenses,

[11] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 7, 2021).

government benefits, medical services, and housing or even give false information to police.

48. According to a recent article in the New York Times, cyber thieves are using driver's licenses obtained via insurance company application prefill processes to submit and fraudulently obtain unemployment benefits.[12] An individual may not know that his or her driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

F. Plaintiff Kristi Hoffman-Mock's Experience

49. Plaintiff Hoffman-Mock received the Defendants' May 28, 2021 Notice of Data Breach on or about that date. The Notice informed her that Defendants lost a file containing at least her full name, Social Security number, date of birth, member identification number, and health insurance information.

50. Shortly after the Data Breach, on or about January 30 and 31, 2021, unknown third parties used Ms. Hoffman-Mock's credit card to make unauthorized purchases via the internet. Then again, on or about April 4 and 13, 2021, unknown third parties used Ms. Hoffman-Mock's credit card to make additional unauthorized purchases via the internet. As of this filing, none of those fraudulent charges have been reimbursed.

51. Moreover, subsequent to the Data Breach, Ms. Hoffman-Mock experienced a significant increase in the amount of suspicious phishing telephone calls she receives. Each day, Plaintiff Hoffman-Mock receives at least two scam phone calls, each of which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

52. Additionally, beginning in or about March 2021, an unknown third party arranged

[12] *How Identity Thieves Took My Wife for a Ride*, New York Times, (April 27, 2021) https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited July 7, 2021)

to have Ms. Hoffman-Mock's U.S. mail diverted from her home address.

53. In response to the Data Breach and the subsequent credit card fraud, Plaintiff Hoffman-Mock 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; contacting her credit card companies regarding the fraudulent charges; contacting the U.S. Postal Service regarding her diverted mail service; dealing with the uptick in unwanted phishing telephone calls; and researching credit monitoring and identity theft protection services.

54. Since signing up for Defendants' free credit monitoring, Ms. Hoffman-Mock reviews her credit monitoring reports and/or checking account statements for irregularities two or three times per week, each time for approximately five minutes. This is valuable time Plaintiff Hoffman-Mock otherwise would have spent on other activities, including but not limited to work and/or recreation.

55. Plaintiff Hoffman-Mock is deeply concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

56. Plaintiff Hoffman-Mock suffered actual injury from having her PII/PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendants obtained from Plaintiff Hoffman-Mock; (b) violation of her privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) actual fraudulent charges on credit cards in her name.

57. As a result of the Data Breach, Plaintiff Hoffman-Mock anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Hoffman-Mock will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

58. Plaintiff brings this nationwide class action pursuant to rules 23(b)(2), 23(b)(3), and

23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> **All natural persons residing in the United States whose PII/PHI was compromised in the Data Breach first announced on or about May 28, 2021 (the "Nationwide Class").**

59. Plaintiff also seeks certification of a Florida sub-class defined as follows:

> **All natural persons residing in the State of Florida whose PII/PHI was compromised in the Data Breach first announced on or about May 28, 2021 (the "Florida Class").**

60. Excluded from the Classes are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

61. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

62. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendants have identified thousands of customers/patients whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendants' records.

63. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendants actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the PII of Plaintiff and members of the Classes;

e. Whether Defendants acted negligently in connection with the monitoring and/or protection of PII belonging to Plaintiff and members of the Classes;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep the PII of Plaintiff and members of the Class secure and to prevent loss or misuse of that PII;

g. Whether Defendants have adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendants caused Plaintiffs' and members of the Classes damage;

i. Whether Defendants violated the law by failing to promptly notify Plaintiff and members of the Classes that their PII had been compromised;

j. Whether Defendants violated the consumer protection statutes invoked below; and

k. Whether Plaintiff and the other members of the Classes are entitled to credit monitoring and other monetary relief.

64. **Typicality**: Plaintiff's claims are typical of those of the other members of the Classes because all had their PII compromised as a result of the Data Breach due to Defendants' misfeasance.

65. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's Counsel are competent and experienced in litigating privacy-related class actions.

66. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

67. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class

Devine Goodman & Rasco, LLP 2800 Ponce De Leon Boulevard, Suite 1400, Coral Gables, Florida 33134 P 305.374.8200 F 305.374.8208

as a whole and as to each Subclass as a whole.

68. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiff and the members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

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

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff, the Nationwide Class, and the Florida Subclass Against All Defendants)

Plaintiff adopts and realleges the allegation contained in Paragraphs 1 – 68 as if fully set forth herein and further states:

69. Defendants owed a duty to Plaintiff and Nationwide Class members to exercise reasonable care in obtaining, using, and protecting their PII and PHI from unauthorized third parties.

70. The legal duties owed by Defendants to Plaintiff and Nationwide Class members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and PHI of Plaintiff and Nationwide Class members in its possession;

b. To protect PII and PHI of Plaintiff and Nationwide Class members in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

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

71. Defendants' duty to use reasonable data security measures also arose under Section 45 CFR 164.306(a)(2), which requires entities that handle PHI "to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information."

72. Defendants breached their duties to Plaintiff and Nationwide Class members. Defendants knew or should have known the risks of collecting and storing PII and PHI and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

73. Defendants knew or should have known that their security practices did not adequately safeguard Plaintiffs' and the other Nationwide Class members' PII and PHI.

74. Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Nationwide Class members' PII and PHI during the period it was within Defendants' possession and control. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect the PII and PHI of Plaintiff and the Classes from being foreseeably captured, accessed, stolen, disclosed, and misused.

75. Defendants breached the duties they owe to Plaintiff and Nationwide Class members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect employees' and customers'/patients PII and thereby creating a foreseeable risk of harm;

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

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

d. Failing to timely and accurately disclose to customers/patients that their PII and PHI had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

76. Due to Defendants' conduct, Plaintiff and Nationwide Class members are entitled to credit monitoring. Credit monitoring is reasonable here. Hackers can use the stolen PII and PHI to engage in financial fraud against the Plaintiff and Nationwide Class members.

77. Some experts recommend that data breach victims obtain credit-monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

78. As a result of Defendants' negligence, Plaintiff and Nationwide Class members suffered injuries that may include, and is not limited to:

a. the lost or diminished value of PII and PHI;

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

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

d. the continued risk to their PII and PHI, which may remain for sale on the dark web and is in Defendants' possession and subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI in their continued possession; and

Devine Goodman & Rasco, LLP 2800 Ponce De Leon Boulevard, Suite 1400, Coral Gables, Florida 33134 P 305.374.8200 F 305.374.8208

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

79. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the Class members suffered was the direct and proximate result of Defendants' negligent conduct.

SECOND CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiff, the Nationwide Class, and the Florida Subclass Against All Defendants)

Plaintiff adopts and realleges the allegation contained in Paragraphs 1 – 68 as if fully set forth herein and further states:

80. Defendants benefited from receiving Plaintiff and Class members' PII and PHI by its ability to retain and use that information for its own benefit. Defendants understood this benefit.

81. Defendants also understood and appreciated that Plaintiff and Class members' PII and PHI was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that PII and PHI.

82. Plaintiff and Class members who were customers of Defendants conferred a monetary benefit upon Defendants in the form of monies paid for services available from Defendants.

83. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class members because they used this information for business purposes.

84. Defendants used the monies that Plaintiff and Class members paid to Defendants for services, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

Devine Goodman & Rasco, LLP 2800 Ponce De Leon Boulevard, Suite 1400, Coral Gables, Florida 33134 P 305.374.8200 F 305.374.8208

85. Defendants also understood and appreciated that Plaintiff and Class Members' PII and PHI was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that PII and PHI.

86. But for Defendants' willingness and commitment to maintain privacy and confidentiality, that PII and PHI would not have entrusted with Defendants. Indeed, if Defendants had informed Plaintiff and Class members that their data and cyber security measures were inadequate, regulators, shareholders, and consumers would not have permitted Defendants to continue to operate in that fashion.

87. Defendants gained unjust enrichment because of their wrongful conduct. This was at the expense of, and to the detriment of, Plaintiff and Class members. Defendants continue to benefit and profit from their retention and use of the PII and PHI while diminishing its value to Plaintiff and Class Members.

88. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this Complaint, including compiling, using, and retaining Plaintiffs' and Class Members' PII and PHI, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

89. Because of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between the amount Plaintiff and Class members paid for their purchases with reasonable data privacy and security practices and procedures and the purchases they actually received with unreasonable data privacy and security practices and procedures.

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

Devine Goodman & Rasco, LLP 2800 Ponce De Leon Boulevard, Suite 1400, Coral Gables, Florida 33134 P 305.374.8200 F 305.374.8208

91. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds they received because of the conduct alleged herein.

THIRD CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of Plaintiff, the Nationwide Class, and the Florida Subclass Against All Defendants)

Plaintiff adopts and realleges the allegation contained in Paragraphs 1 – 68 as if fully set forth herein and further states:

92. Plaintiff and Class Members had a legitimate expectation of privacy with regard to their PII and PHI. They are entitled to the protection of this information against disclosure to unauthorized third parties.

93. Defendants owed a duty to Plaintiff and Class Members to keep their PII and PHI confidential.

94. Defendants failed to protect patient PII and PHI by allowing a hacker to gain access to the Plaintiff and Class Member's data.

95. A reasonable person would find the unauthorized release of PII and PHI highly offensive.

96. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members gave Defendants their PII and PHI with the understanding that the information would remain confidential.

97. The Data Breach that occurred because of the Defendant's actions caused an intentional interference with Plaintiff's and Class Members interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a type that would be highly offensive to a reasonable person.

98. Defendants acted knowingly when they allowed the Data Breach to occur because they had actual knowledge that their cyber-security practices were not adequate. As such,

Devine Goodman & Rasco, LLP 2800 Ponce De Leon Boulevard, Suite 1400, Coral Gables, Florida 33134 P 305.374.8200 F 305.374.8208

Defendants had notice and knew that the inadequate cyber-security practices would cause injury and harm to Plaintiff and Class Members.

99. Plaintiff and Class Members suffered damages as a proximate result of Defendants' acts and omissions when they disclosed to a third party, without authorization, the PII and PHI.

100. The Defendants wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members unless Defendants are enjoined and restrained by order of this court.

FOURTH CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiff, the Nationwide Class, and the Florida Subclass Against All Defendants)

Plaintiff adopts and realleges the allegation contained in Paragraphs 1 – 68 as if fully set forth herein and further states:

101. As a condition of using Defendants' services, Plaintiff and Class Members were required to provide their PII and PHI.

102. With a reasonable expectation that Defendants would protect their PII and PHI, Plaintiff and Class Members paid Defendants directly or indirectly.

103. There was an implicit agreement between the Defendants and its patients, which includes Plaintiff and Class Members, that Defendants would protect the PII and PHI of its patients. Defendants had an obligation to use the PII and PHI for business purposes only and to take reasonable steps to secure and safeguard the PII and PHI from others gaining unauthorized access to this sensitive information. Also implicit in the agreement was an obligation to provide Plaintiff and Class Members with prompt notice of any breach that gave access to PII and PHI to unauthorized people. Plaintiff and Class Members would not have provided Defendants with their PII and PHI without an implied contract.

104. There was an implied duty that Defendants would safeguard the PII and PHI of Plaintiff and Class Members from unauthorized disclosure or use.

105. Due to the nature of the relationship between Defendants and Plaintiff and Class Members, there was an implicit promise to keep the PII and PHI confidential and secure.

106. Plaintiff and Class Members fully performed their obligations under the implied contract when they provided their PII and PHI to Defendants.

107. Defendants did not fully perform their obligations under the implied contract when they did not secure the PII and PHI of Plaintiff and Class Members and failing to comply with HIPAA.

108. Defendants did not fully perform their obligations under the implied contract when they violated 45 CFR 164.306(a)(1) by failing to ensure the confidentiality and integrity of Plaintiff and Class Members' protected electronic health information that Defendants created, received, maintained, and transmitted.

109. Defendants did not fully perform their obligations under the implied contract when they violated 45 CFR 164.312(a)(1) by failing to implement technical policies and procedures for their electronic information systems that housed the PII and PHI of Plaintiff and Class Members. Only those people who have authorized access to the protected PII and PHI are allowed to access the information, which was clearly not the case in this breach.

110. Defendants did not fully perform their obligations under the implied contract when they violated 45 CFR 164.308(a)(1) by failing to implement policies and procedures to prevent, detect, contain, and correct security violations.

111. Defendants did not fully perform their obligations under the implied contract when they violated 45 CFR 164.308(a)(6)(ii) by failing to mitigate, to the extent practicable, harmful effects of security incidents that were known to Defendants.

112. Defendants did not fully perform their obligations under the implied contract when they violated 45 CFR 164.306(a)(2) by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI.

FIFTH CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On Behalf of Plaintiff, the Nationwide Class,
and the Florida Subclass Against All Defendants)

Plaintiff adopts and realleges the allegation contained in Paragraphs 1 – 68 as if fully set forth herein and further states:

113. The Defendants had a fiduciary duty with their patients, which include Plaintiff and Class Members, because Defendants were guardians of highly sensitive and confidential information about the Plaintiff and Class Members. Defendants had a fiduciary duty to Plaintiff and Class Members to safeguard their PII and PHI, adequately notify them of the data breach, and maintain complete records of what information was stored and/or deleted.

114. Defendants breached this duty when they did not protect the systems in which they stored Plaintiff and Class Members' PII and PHI.

115. Defendants breached this duty when they did not provide adequate notification of the data breach by providing vague descriptions of stolen PII and PHI and by waiting too long to provide notice of the breach to Plaintiff and Class Members.

116. Defendants breached their fiduciary duty when they violated 45 CFR 164.306(a)(1) by failing to ensure the confidentiality and integrity of Plaintiff and Class Members' protected electronic health information that Defendants created, received, maintained, and transmitted.

117. Defendants breached their fiduciary duty when they violated 45 CFR 164.312(a)(1) by failing to implement technical policies and procedures for their electronic information systems that housed the PII and PHI of Plaintiff and Class Members. Only authorized individuals are allowed to access the protected PII and PHI, which was clearly not the case in this breach.

118. Defendants breached their fiduciary duty when they violated 45 CFR 164.308(a)(1) by failing to implement policies and procedures to prevent, detect, contain, and correct security violations.

Devine Goodman & Rasco, LLP 2800 Ponce De Leon Boulevard, Suite 1400, Coral Gables, Florida 33134 P 305.374.8200 F 305.374.8208

119. Defendants breached their fiduciary duty when they violated 45 CFR 164.308(a)(6)(ii) by failing to mitigate, to the extent practicable, harmful effects of security incidents that were known to Defendants.

120. Defendants breached their fiduciary duty when they violated 45 CFR 164.306(a)(2) by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI.

121. Defendants breached their fiduciary duty when they violated 45 CFR 164.306(a)(3) by failing protect Plaintiff and Class Members' PHI and PII from any reasonably-anticipated uses or disclosures that are not permitted under the privacy rules regarding PHI.

122. Defendants breached their fiduciary duty when they violated 45 CFR 164.306(a)(94) by failing to ensure their workforce complied with HIPAA security standard rules.

123. Defendants breached their fiduciary duty when they violated 45 CFR 164.502, et seq. by impermissibly and improperly using and disclosing PHI that remains accessible to unauthorized people.

124. Defendants breached their fiduciary duty when they violated 45 CFR 164.530(b) and 45 CFR 164.308(a)(5) by failing to provide adequate training to their workforce on the policies and procedures with respect to PHI so that their workforce could carry out their function and maintain security of the PHI they handled.

125. Defendants breached their fiduciary duty when they violated 45 CFR 164.530(c) by failing to design, implement, and enforce policies and procedures to establish a physical and administrative safeguard to protect PHI.

126. Plaintiff and Class Members face injuries as a direct and proximate result of Defendants' breaches of their fiduciary duties. These injuries include, but are not limited to:

a. Actual identity theft;

b. Loss of control over their PII and PHI;

c. The publication and compromise of their PII and PHI;

Devine Goodman & Rasco, LLP 2800 Ponce De Leon Boulevard, Suite 1400, Coral Gables, Florida 33134 P 305.374.8200 F 305.374.8208

d. Expenses related to protecting themselves from further fraud now that their PII and PHI is available on the dark web;

e. Lost opportunity costs associated with spending time on protecting themselves from future fraud when they could be doing something else;

f. A continued risk that Plaintiff and Class Members PII and PHI could be stolen from Defendants care again in the future;

g. Future costs associated with spending time on protecting themselves from any future fraud as a result of the compromised PII and PHI;

h. A diminished value of Defendants' services received by Plaintiff and Class Members; and

i. Anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SIXTH CLAIM FOR RELIEF
Breach of Confidence
(On Behalf of Plaintiff, the Nationwide Class, and the Florida Subclass Against All Defendants)

Plaintiff adopts and realleges the allegation contained in Paragraphs 1 – 68 as if fully set forth herein and further states:

127. Defendants were aware of the confidential nature of handling the PII and PHI of Plaintiff and Class Members at all times.

128. As alleged above, there was an expectation in the relationship between Defendants and Plaintiff and Class Members that unauthorized people would not be able to gain access to the PII and PHI collected and stored by Defendants.

129. There was an explicit and implicit understanding that Defendants would protect the PII and PHI of Plaintiff and Class Members from unauthorized people by taking precautions to protect this data.

130. Defendants voluntarily received the PII and PHI of Plaintiff and Class Members with the understanding that it would remain private and safe from unauthorized access.

Devine Goodman & Rasco, LLP 2800 Ponce De Leon Boulevard, Suite 1400, Coral Gables, Florida 33134 P 305.374.8200 F 305.374.8208

131. Defendants failed to prevent, detect, and avoid the Data Breach by failing to implement best information security practices. This failure led to the misappropriation of the PII and PHI of Plaintiff and Class members by unauthorized people.

132. Plaintiff and Class Members suffered damages as a direct and proximate cause of Defendants' actions and or omissions.

133. But for Defendants conduct, the PII and PHI would not have been compromised, stolen, viewed, accessed, deleted, and used by unauthorized people. This is in violation of the parties' understanding of confidence. The direct and legal cause of the theft of the PII and PHI is the Data Breach and resulting damages allowed by Defendants conduct.

134. Plaintiff and Class Members suffered injury and harm, which was the foreseeable result of Defendants' unauthorized disclosure of PII and PHI. Defendants failed to implement basic security practices necessary to prevent people from creating fraudulent provider accounts. As such, Defendants knew or should have known that the 20/20 computer systems were not secure.

135. As a direct and proximate result of Defendants' breach of confidence, Plaintiff and Class Members suffered injury, including but not limited to:

a. Actual identity theft;

b. Loss of control over their PII and PHI;

c. The publication and compromise of their PII and PHI;

d. Expenses related to protecting themselves from further fraud now that their PII and PHI is available on the dark web;

e. Lost opportunity costs associated with spending time on protecting themselves from future fraud when they could be doing something else;

f. A continued risk that Plaintiff and Class Members PII and PHI could be stolen from Defendants care again in the future;

g. Future costs associated with spending time on protecting themselves from any future fraud as a result of the compromised PII and PHI;

h. A diminished value of Defendants' services received by Plaintiff and Class Members; and

Devine Goodman & Rasco, LLP 2800 Ponce De Leon Boulevard, Suite 1400, Coral Gables, Florida 33134 P 305.374.8200 F 305.374.8208

i. Anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SEVENTH CLAIM FOR RELIEF
Violations of the Florida Unfair and Deceptive Trade Practices Act, Fla. Stat. §§ 501.201, *et seq*.
(On Behalf of Plaintiff, the Nationwide Class, and the Florida Subclass Against All Defendants)

Plaintiff adopts and realleges the allegation contained in Paragraphs 1 – 68 as if fully set forth herein and further states:

136. Plaintiff and Class Members purchased or otherwise availed themselves of insurance benefits from 20/20 for personal, family, or household purposes.

137. Defendants engaged in transactions and conduct to procure health-related services on behalf of Plaintiff and Class Members.

138. Defendants engaged in trade and commerce through its acts and omissions and its course of business, including marketing, offering to sell, and selling health services throughout the United States.

139. Defendants violated Fla. Stat. section 501.204(1) by engaging in deceptive, unfair, and unlawful trade acts or practices while conducting trade or commerce in Florida. Defendants violations include, but are not limited to:

a. A failure to safeguard patient-customer PII and PHI through data security practices and computer systems;

b. A failure to disclose that their computer systems and data security practices were inadequate to protect PHI and PII;

c. A failure to notify Plaintiff and Class Members in a timely manner of the data breach;

d. A failure to stop accepting and storing patient PII and PHI after the Defendants knew or should have known that the vulnerabilities were exploited in a data breach; and

e. A failure to remediate the vulnerabilities that allowed the Data Breach to happen.

140. These unfair acts and practices violate the duties imposed by, but not limited to, the FTCA and Fla. Stat. section 501.171(2).

141. As a direct result of these violations, Plaintiff and Class Members suffered damages. These damages include, but are not limited to:

a. Lost time spent constantly checking their credit for unauthorized activity, which is necessary to do to protect themselves from the consequences of having their PII and PHI available on the dark web because of the Data Breach; and

b. Other economic damage that may not be detected for years to come.

142. Plaintiff and Class Members are entitled to damages as well as injunctive relief because of Defendants' knowing violation of Florida Unfair and Deceptive Trade Practices Act. These include, but are not limited to, ordering that defendants:

a. Utilize third-party security professionals to regularly test for security vulnerabilities;

b. Utilize third-party security professionals and internal personnel to perform automated security monitoring;

c. Train security personnel on how to audit and test any new or modified security protocols;

d. Protect patient data by securing it separately from other portions of the network;

e. Delete patient PII and PHI that is no longer necessary to provide services;

f. Conduct regular database security checks;

g. Provide regular training to internal security personnel on how to identify and contain a breach and what to do when a breach occurs; and

h. Educate patients about the threats they face now that their PII and PHI is available to unauthorized third parties and steps that patients can take to protect themselves.

143. Plaintiff brings this action on behalf of herself and Class Members for the relief requested above. This action will also protect the public from Defendants unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices.

144. The deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. The acts caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid and the injuries suffered outweigh any benefit to patient-consumers or to competition.

145. Defendants knew or should have known that the computer systems and data security protocols were inadequate to store sensitive PII and PHI, which put the data at an increased risk of theft or breach.

146. Defendants' unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless.

147. Plaintiff and Class Members seek relief under the Florida Deceptive and Unfair Trade Practices Act (Fla. Stat. §§ 501.201). The relief includes, but is not limited to, damages, restitution, injunction relief, and/or attorney fees and costs, and any other just and proper relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Nationwide Class members, requests judgment against the Defendants and that the Court grant the following:

A. An order certifying the Classes as defined herein, and appointing Plaintiff and their counsel to represent the Classes;

B. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII and PHI belonging to Plaintiff and the members of the Classes;

C. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiff and all members of the Classes;

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

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

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

G. Such other and further relief as this Court may deem just and proper.

Devine Goodman & Rasco, LLP 2800 Ponce De Leon Boulevard, Suite 1400, Coral Gables, Florida 33134 P 305.374.8200 F 305.374.8208

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated this 8th, day of July 2021.

Respectfully submitted,

DEVINE GOODMAN & RASCO, LLP
2800 Ponce de Leon Blvd., Suite 1400
Coral Gables, FL 33134
Tel: 305-374-8200
Email: rkuntz@devinegoodman.com

/s/ Robert J. Kuntz, Jr.
Robert J. Kuntz Jr., Esq.
Fla. Bar No: 094668

And Co-Counsel

M. Anderson Berry, Esq.
Alex Sauerwein, Esq.
(*Pro Hac Vice application forthcoming*)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Tel: (916) 777-7777
aberry@justice4you.com
asauerwein@justice4you.com

Attorneys for Plaintiff and the Class

Save As... Print Reset

JS 44 (Rev. 10/20) FLSD Revised 02/12/2021

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)* **NOTICE: Attorneys MUST Indicate All Re-filed Cases Below.**

I. (a) PLAINTIFFS

KRISTI HOFFMAN-MOCK, individually and o

DEFENDANTS

20/20 EYE CARE NETWORK, INC., and ICAF

(b) County of Residence of First Listed Plaintiff Marion County
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Robert J. Kuntz, Jr., Devine Goodman & Rasco, LLP, 2800 Ponce De L

Attorneys *(If Known)*

(d) Check County Where Action Arose: ☐ MIAMI- DADE ☐ MONROE ☐ BROWARD ☐ PALM BEACH ☐ MARTIN ☐ ST. LUCIE ☐ INDIAN RIVER ☐ OKEECHOBEE ☐ HIGHLANDS

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff) and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excl. Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Med. Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Mgmt. Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Empl. Ret. Inc. Security Act

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent – Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729 (a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act (TCPA)
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence

Other:
- ☐ 530 General
- ☐ 535 Death Penalty
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee – Conditions of Confinement

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Re-filed **(See VI below)** ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district *(specify)* ☐ 6 Multidistrict Litigation Transfer ☐ 7 Appeal to District Judge from Magistrate Judgment ☐ 8 Multidistrict Litigation – Direct File ☐ 9 Remanded from Appellate Court

VI. RELATED/ RE-FILED CASE(S)

(See instructions): a) Re-filed Case ☐ YES ☐ NO b) Related Cases ☒ YES ☐ NO

JUDGE: Rodolfo A. Ruiz, II **DOCKET NUMBER:** 0:21-cv-61275-RAR

VII. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing and Write a Brief Statement of Cause ***(Do not cite jurisdictional statutes unless diversity)***:

28 U.S.C. § 1332(d)(2)

LENGTH OF TRIAL via days estimated (for both sides to try entire case)

VIII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A **CLASS ACTION** UNDER F.R.C.P. 23

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

ABOVE INFORMATION IS TRUE & CORRECT TO THE BEST OF MY KNOWLEDGE

DATE SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY : RECEIPT # **AMOUNT** IFP JUDGE MAG JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. (a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.C.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked. Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; federal question actions take precedence over diversity cases.)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.

Original Proceedings. (1) Cases which originate in the United States district courts.

Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.

Refiled (3) Attach copy of Order for Dismissal of Previous case. Also complete VI.

Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

Appeal to District Judge from Magistrate Judgment. (7) Check this box for an appeal from a magistrate judge's decision.

Remanded from Appellate Court. (8) Check this box if remanded from Appellate Court.

VI. Related/Refiled Cases. This section of the JS 44 is used to reference related pending cases or re-filed cases. Insert the docket numbers and the corresponding judges name for such cases.

VII. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity**. Example: U.S. Civil Statute: 47 USC 553
Brief Description: Unauthorized reception of cable service

VIII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.

Demand. In this space enter the dollar amount (in thousands of dollars) being demanded or indicate other demand such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

Kristi Hoffman-Mock, individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

20/20 EYE CARE NETWORK, INC., and ICARE HEALTH SOLUTIONS, LLC,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* 20/20 EYE CARE NETWORK, INC.
c/o Resgistered Agent
PATRICE TREAS COPPOLA
2900 W. CYPRESS CREEK
FORT LAUDERDALE, FL 33309

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Robert J. Kuntz, Jr., Esq.
Devine Goodman & Rasco, LLP
2800 Ponce De Leon Blvd., Suite 1400
Coral Gables, FL 33134
Ph: 305-374-8200

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

Kristi Hoffman-Mock, individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

20/20 EYE CARE NETWORK, INC., and ICARE HEALTH SOLUTIONS, LLC,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* ICARE HEALTH SOLUTIONS, INC.
CORPORATION SERVICE COMPANY
1201 HAYS STREET
TALLAHASSEE, FL 32301

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Robert J. Kuntz, Jr., Esq.
Devine Goodman & Rasco, LLP
2800 Ponce De Leon Blvd., Suite 1400
Coral Gables, FL 33134
Ph: 305-374-8200

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset

ClassAction.org