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

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

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,

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.