Alex R. Straus, SBN 321366
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
(917) 471-1894 (phone)
(615) 921-6501 (fax)
astraus@milberg.com

Plaintiffs' Attorneys

Additional attorneys on signature page

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

VICKEY ANGULO, individually and on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

SUPERCARE HEALTH, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

Demand for Jury Trial

Plaintiff Vickey Angulo ("Plaintiff") brings this Complaint against Defendant SuperCare Health, Inc. ("SCH"), individually and on behalf of all others similarly situated, and alleges upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. On or about March 25, 2022, SCH posted a notice, entitled Notice of Data Breach (hereinafter, the "Notice"), announcing publicly that an unauthorized actor accessed SCH's files.

2. According to SCH's Notice, current and former patients' personally identifiable information ("PII") and protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including, but not limited to, patients' names, addresses, dates of birth, hospital or medical group, patient account numbers, medical record numbers, health insurance information, testing/diagnostic/treatment information, and other health-related information, as well as, for some, Social Security numbers and driver's license numbers (collectively, the "Private Information"), were accessed and compromised by an unauthorized third party in the cybersecurity incident (the "Data Breach").

3. As detailed below, the Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and the Class Members' Private Information despite the fact that data breach attacks against medical systems and healthcare providers are at an all-time high.

4. This attack enabled an unauthorized third-party to access SCH's computer systems and the highly sensitive and confidential data of thousands of current and former patients of SCH, including Plaintiff.

5. Plaintiff received a notification letter from SCH informing her that the information accessed by the third-party actors included her electronic health records.

6. SCH, despite professing to take the privacy and security of its patients' confidential and health information seriously, has not offered to provide affected individuals with adequate credit monitoring service or compensation for the damages they have suffered as a result of the Breach.

7. As a consequence of the Data Breach, Plaintiff's and Class members' Private Information has been released into the public domain and they have had to, and will continue to have to, spend time to protect themselves from fraud and identity theft.

8. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, through frequent news reports and FBI warnings to the healthcare industry, and thus it was on notice that failing to take steps necessary to secure the Private Information from those risks left the property in a dangerous and vulnerable condition.

9. Defendant disregarded the rights of Plaintiff's and Class Members (defined below) by, inter alia, intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Private Information; failing to take standard and reasonably available steps to prevent the Data Breach and failing to provide Plaintiff and Class Members accurate notice of the Data Breach.

10. Plaintiff's and Class Members' identities are now at risk because of Defendant's conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class

Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph and/or giving false information to police during an arrest.

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

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

14. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

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.