Jonathan M. Lebe (State Bar No. 284605)
Jon@lebelaw.com
Zachary Gershman (State Bar No. 328004)
Zachary@lebelaw.com
Shigufa Saleheen (State Bar No. 341013)
Shigufa@lebelaw.com
**Lebe Law, APLC**
777 S. Alameda Street, Second Floor
Los Angeles, CA 90021
Telephone: (213) 444-1973

Attorneys for Plaintiff Harmon Cottrell,
Individually and on behalf of all others similarly situated

**UNITED STATES DISTRICT COURT**

**CENTRAL DISTRICT OF CALIFORNIA**

Harmon Cottrell, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

Super Care, Inc., d/b/a SuperCare Health, Inc.,

Defendant.

**CLASS ACTION COMPLAINT**

DEMAND FOR JURY TRIAL

## NATURE OF ACTION AND INTRODUCTORY STATEMENT

1. Plaintiff Harmon Cottrell ("Plaintiff") brings this class action against Defendant SuperCare Health, Inc. ("Defendant") for its failure to properly secure and safeguard personally identifiable information ("PII") and protected health information ("PHI") of its patients.

2. Defendant SuperCare Health, Inc. ("Defendant") is a "leading post-acute, in-home respiratory care provider in the Western U.S."[1] with the goal "to be the most trusted partner managing high-risk respiratory diseases combining both in-home, high-touch care with telehealth and remote monitoring."[2]

3. As a corporation doing business in California, Defendant is legally required to protect PII and PHI from unauthorized access and exfiltration.

4. According to Defendant's Notice of Security Incident on its website, Defendant first noticed "unauthorized activity" on its systems on July 27, 2021.[3] A subsequent forensic investigation revealed that an unknown party had access to certain systems on Defendant's network from July 23, 2021 to July 27, 2021 ("Data Breach").[4]

5. Defendant did not report this Data Breach to the Health and Human Services Office of Civil Rights ("OCR") until March 28, 2022[5] – nearly eight months after Defendant originally became aware of the breach.

6. Between July 2021 and March 2022, Plaintiff and other similarly situated Class Members were unaware that their personally identifiable information ("PII") and protected health information ("PHI") had been potentially compromised. The potentially affected data includes, but is not limited to, "name, address, date of birth, hospital or medical group, patient account number, medical record number, health

---

[1] https://supercarehealth.com (last visited May 18, 2022).
[2] https://supercarehealth.com/homepage/who-we-are/overview/ (last visited May 18, 2022).
[3] https://supercarehealth.com/supercareprotects/ (last visited May 18, 2022).
[4] *Id.*
[5] *See* U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information ("Breach Portal"), available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited May 18, 2022).

insurance information, testing/diagnostic/treatment information, other health-related information, and claim information."[6] Defendant reports that for a small subset of individuals, the patient's "Social Security number and/or driver's license number may have been contained in the impacted files."[7]

7. According to the OCR HIPPA Breach Reporting Tool, the breach affected nearly 318,400 current and former patients of Defendant.[8]

8. When Defendant finally notified Plaintiff and Class Members of the breach on March 25, 2022, Defendant failed to explain why its failed to prevent the hack for four days, why it did not immediately notify potentially affected individuals so they may be able to protect their data, or why its internal investigation of the incident took nearly six months.

9. In response to the Data Breach, Defendant claims that it "implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents."[9] However, Defendant fails detail how its previous security systems gave rise to the Data Breach, or share any tangible information regarding the steps taken in order to further secure this highly sensitive information.

10. According to Defendant's Privacy Policy[10], Defendant upholds that patient "protected health information," as well as "any additional unique personally identifiable information … is not transferred to any third party."

11. However, despite its own promise to Plaintiff and Class Members, Defendant failed to safeguard and protect this information from unauthorized access and disclosure.

---

[6] *See* Notice Of Data Security Incident, available at: https://supercarehealth.com/supercareprotects/ (last visited May 18, 2022).

[7] *See Id.*

[8] *See* Breach Portal; *see also* SuperCare Health Sued for PHI Breach Affecting 318,000, available at: https://thehipaaetool.com/supercare-health-sued-for-phi-breach-affecting-318000/ (last visited May 18, 2022).

[9] *See* Notice of Data Security Incident

[10] *See* SuperCare Health Privacy Policy, available at: https://supercarehealth.com/homepage/privacy-policy/ (last visited May 18, 2022).

12. As a result of Defendant's failure to provide reasonable and adequate data security, Plaintiff's and Class Members' PII and PHI have been exposed to those who should not have access to it. As a result, Plaintiff and putative class members are now at much higher risk of identity theft and for cybercrimes, especially considering the highly valuable, sensitive, and sought-after PII and PHI stolen here.

13. The PII and PHI exposed by Defendant as a result of its inadequate data security is highly valuable on the black market to phishers, hackers, identity thieves, and cybercriminals. Stolen PII and PHI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity. PHI and medical records, are of significantly high value to cybercriminals, with reports that the information could go for up to $1,000 on the dark web.[11]

14. When malicious actors infiltrate companies and copy and exfiltrate the PII and PHI that those companies store, or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.

15. Here, the information potentially compromised by the Data Breach is difficult and highly problematic to change— such as driver's license numbers, social security numbers, and addresses.

16. Unauthorized data breaches, such as these, facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

17. Moreover, Plaintiff's and the Class Members's PHI is highly coveted and protected under the Health Insurance Portability and Accountability Act of 1996

[11] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited May 18, 2022).

("HIPAA"). Due to Defendant's negligence resulting in this Data Breach, Plaintiff and Class Members' medical hospital information, patient account numbers, medical record numbers, health insurance numbers, testing/diagnostic/treatment information, and claim information have all been compromised. All of this information can be utilized to facilitate medical identity theft. Thus, ss a result of Defendant's negligence and this Data Breach, Plaintiff and Class Members face a heighted risk of having false medical and health insurance claims made under their names, receiving bills for medicine and treatments these patients' did not actually receive, and experiencing disruptions or fraudulent changes made to their medical records.

18. Notably, once PII and PHI is compromised or stolen, it cannot be recovered or returned to an uncompromised condition—these individuals do not even have the ability to stop future unlawful usage from occurring. As such, Plaintiff and Class Members must remain vigiliant, in perpetuity, to ensure that their PII and PHI is not being fraudulently used.

19. Defendant was obligated under the HIPAA, contract law, industry standards, common law and its own representations made to Plaintiff and Class Members to keep their PII and PHI confidential.

20. Ultimately, Plaintiff's and Class Member's PII and PHI were compromised due to Defendant's own negligent acts and omissions, as well as its failure to adequately safeguard this crucial information.

21. On information and belief, Defendant's systems were inadequate to detect and prevent the "unauthorized activity" that led to the Data Breach, as the information was not stored in an encrypted protected manner as required by reasonable standards.

22. As a result of Defendant's negligence resulting in this Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages including, but not limited to, monetary losses and economic harm, invasion of privacy,

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.