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,

an indefinite increased risk of personal identity and medical identity theft, heighted nusiances due to compromised personal contact information, and emotional distress.

23. Specifically, as a result of this unauthorized Data Breach, Plaintiff has spent a considerable time and effort monitoring his information to determine if he has been subject to any data breaches. Plaintiff reports experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach, due to the unknown nature of what information was compromised to what extent.

24. Further, Plaintiff believes that there may have been more PII compromised that what is reported by Defendant. Specifically, after the Data Breach, Plaintiff reports receiving an influx of scam calls and text messages to his personal cell phone— which is unlisted and unaccessible online. These nuisance calls add regular and consistent interruptions into Plaintiff's day and trigger constant reminders of the potential PII and PHI that has been exposed as a result of this Data Breach. As such, this goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

25. Further, as a result of the unauthorized data disclosure, Plaintiff and Class Members are now at risk for actual identity and medial identity theft in addition to other forms of fraud. The ramifications of Defendant's failure to keep PII and PHI secure are long lasting and severe. The PII belonging to Plaintiff and class members is private, valuable, and sensitive in nature as it can be used to commit a variety of harms in the hands of the wrong people.

26. In response to the exposure of this sensitive PII and PHI, Defendant only offers Plaintiff and Class Members up to 12 months of free credit monitoring. Not only is this insufficient to remedy the lifelong identity theft threat that each patient now faces, it completely fails to remedy the exposure of of Plaintiff and Class Members' highly sensitive protected health information—the illicit usage of which cannot be monitored.

27. Defendant had ample resources necessary to prevent the unauthorized data disclosure, but neglected to adequately implement data security measures, despite its obligations to protect the PI of Plaintiff and putative class members. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the unauthorized access of PII and PHI.

28. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and putative class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the unauthorized data disclosure on their lives.

JURISDICTION AND VENUE

29. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d), as the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant.

30. The United States District Court for the Central District of California has personal jurisdiction over Defendant because Defendant is headquartered in this District and does substantial business in California.

31. Venue is proper because Defendant is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

THE PARTIES

32. Plaintiff was a patient of SuperCare Health, Inc, where he frequently purchased medical equipment for his respiratory needs. On March 25, 2022, Plaintiff received a notice from Defendant regarding the breach of his personal information,

including "name, address, date of birth, patient account number, health insurance policy/member number, diagnostic information, treatment information, physician's name, and claim information."

33. Defendant Super Care, Inc. d/b/a SuperCare Health, Inc., is a California corporation with its headquarters in Downey, California.

34. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

35. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

CLASS ACTION ALLEGATIONS

36. Plaintiff seeks relief on behalf of himself and as a representative of all others who are similarly situated.

(a) Nationwide Class: All individuals nationwide whose PII or PHI was actually or potentially compromised during the data breach referenced in the Notice of Data Breach sent by Defendant on or around March 25, 2022.

(b) California Class: All individuals residing in California whose PII or PHI was actually or potentially compromised during the data breach referenced in the Notice of Data Breach sent by Defendant on or around March 25, 2022.

37. Plaintiff reserves the right to amend the class definition.

38. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

(a) Numerosity: The Class Members are believed to be so numerous and geographically dispersed that the joinder of all members is

impractical. Upon information and belief, the number of potentially affected individuals is over 300,000.

(b) Commonality: Plaintiff and the Class Members's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members, such as:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and Class Member's PII and PHI;

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

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII and PHI;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and Class Member's PII and PHI;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable; and

vii. Whether the Data Breach caused Plaintiff and Class Members injuries.

(c) Typicality: Plaintiff's claims and damages sought are typical of those of other Class Members. Further, Plaintiff seeks relief consistent with the relief sought by Class Members.

(d) Adequacy of Representation: Plaintiff will fairly and adequately protect the proposed Class's interests, and his interests do not conflict with Class members' interests.

///

///

FIRST CAUSE OF ACTION

VIOLATION OF CALIFORNIA'S CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA")

(Cal. Civ. Code § 56.10, *et seq.*)

(on behalf of Plaintiff and the California Class)

39. Pursuant to the Confidentiality of Medical Information Act, Cal. Civ. Code § 56.10 *et seq*, "a provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization."

40. Under Cal. Civ. Code § 56.101(a), "Every provider of health care… or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." Any entity "who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36."

41. Moreover, under Cal. Civ. Code § 56.05(a), "any business organized for the purpose of maintaining medical information … in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual, shall be deemed to be a provider of health care subject to the requirements of this part."

42. Here, Defendant provided in-home respiratory care services for its patients through a "team of specialized RTs, RNs, pharmacists, and RDs, together with high-tech solutions with mobile apps, telehealth, and video education."[12] As

[12] https://supercarehealth.com/homepage/who-we-serve/physicians-specialty-groups/

such, under Cal. Civ. Code § 56.05(m), Defendant operates as a provider of health care as to Plaintiff and Class Members.

43. Moreover, Defendant maintained medical information within its systems for the purpose of providing medical equipment, telehealth appointments, prescription refills, and app-based health care data management. To the extent that Defendant may be only providing medical supplies to Plaintiff and Class Members, Defendant still qualifies as a medical services organization that qualifies as a "contractor" of health care services under Cal. Civ. Code § 56.05(d), and must be held to the standards reflected in this statute.

44. Under Cal. Civ. Code 56.05(l), "medical information" refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care… or contractor regarding a patient's medical history, mental or physical condition, or treatment." Further, "individually identifiable" refers to "medical information [that] includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual."

45. Here, Defendant maintained, preserved, and stored Plaintiff's and the California Class's "medical information," as defined under Cal. Civ. Code § 56.05(l), such as testing/diagnostic/treatment information, other health-related information, and claim information. This information — coupled with individually identifiable information regarding the Plaintiff and the California Class, such as names, addresses, and dates of birth — together, could reveal the identity of Plaintiff and the California Class.

46. Under Cal. Civ. Code § 56.05(j), a "patient" refers to "a natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains." Here, Plaintiff and the

California Class are "patients" as defined by Cal. Civ. Code § 56.05(k) because they receive medical treatment and services from Defendant and its health care partners, and the medical information implicated in this Data Breach are directly related to them.

47. Thus, as Defendant is bound by CIMA standards, Defendant owed a duty to preserve the confidentiality of Plaintiff's and the California Class's medical information and to not allow their medical information to be released and viewed by unauthorized persons.

48. Defendant breached its duty owed to Plaintiff and the California Class by failing to implement fair, reasonable, or adequate computer systems and data security policies to safeguard Plaintiff's and California Class Members' medical information, and by allowing that PHI to be released and viewed by unauthorized persons.

49. The resulting unauthorized access and potential acquisition of Plaintiff's and California Class Members' PHI to unauthorized hackers during the Data Breach was an affirmative communicative act in violation of Cal. Civ. Code § 56.101(a). Further, Plaintiff's and California Class Members' PHI was viewed by the unauthorized hackers as a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56.101(a).

50. Further, Plaintiff's and California Class Members' PHI that was subject to the Data Breach included "electronic medical records" or "electronic health records" as referenced by Cal. Civ. Code § 56.101(c).

51. Under Cal. Civ. Code § 56.101(b)(1)(A), a proper electronic health record system or electronic medical record system must "[p]rotect and preserve the integrity of electronic medical information." Here, Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information, which ultimately resulted in Plaintiff's and California Class Members' PHI being viewed by unauthorized hackers in the Data Breach. Thus, the Data

Breach was a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56.101.

52. Under Cal. Civ. Code § 56.101(b)(1)(B), a proper electronic health record system or electronic medical record system must "[a]utomatically record and preserve any change or deletion of any electronically stored medical information. The record of any change or deletion shall include the identity of the person who accessed and changed the medical information, the date and time the medical information was accessed, and the change that was made to the medical information."

53. Here, Defendant's electronic health record system or electronic medical record system failed to automatically record and preserve any actual or potential change or deletion of any electronically stored medical information, in violation of Cal. Civ. Code § 56.101(b)(1)(B).

54. Further, Defendant's electronic health record system or electronic medical record system failed to record the identity of persons who actually or potentially accessed and changed medical information, failed to record the date and time medical information was accessed and failed to record any actual or potential changes that were made to medical information, in violation of Cal. Civ. Code § 56.101(b)(1)(B).

55. Under Cal. Civ. Code § 56.10(e), a health care provider "shall not further disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan or insurer or self-insured employer received under this section to a person or entity that is not engaged in providing direct health care services to the patient or his or her provider of health care or health care service plan or insurer or self-insured employer."

56. Here, Defendant disclosed Plaintiff's and California Class Members' PHI to persons or entities not engaged in providing direct health care services to Plaintiff's or California Class Members or their providers of health care or health

care service plans or insurers or self-insured employers, in violation of § 56.10(e).

57. The foregoing violations of CMIA resulted from Defendant's affirmative actions, and Defendant knew or should have known it had inadequate computer systems and data security practices to safeguard such information. Defendant knew or should have known of the risks inherent in collecting and storing the protected medical information of Plaintiff and members of the California Class.

58. The injury and harm Plaintiff and members of the California Class suffered was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and its breach would cause Plaintiff and members of the California Class to suffer the foreseeable harms associated with the exposure of their PHI.

59. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and members of the California Class now face an increased risk of future harm.

60. Under Cal. Civ. Code § 56.36(b), an individual may bring an action against a person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: "(1) … nominal damages of one thousand dollars ($1,000). In order to recover under this paragraph, it is not necessary that the plaintiff suffered or was threatened with actual damages" and "(2) The amount of actual damages, if any, sustained by the patient."

61. Here, Defendant negligently released confidential information or records concerning Plaintiff's and California Class Members' PHI in violation of Cal. Civ. Code § 56.36(b). As such, Plaintiff and California Class Members are entitled to bring an action for damages against Defendant.

62. As a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56, et seq., Plaintiff and members of the California Class have suffered injury and are entitled to damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION

VIOLATION OF CALIFORNIA CONSUMER RECORDS ACT

Cal. Bus. Code § 1798.80, *et seq*.

(on behalf of Plaintiff and the California Class)

63. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

64. California Civil Code section 1798.80, *et seq.*, known as the "Customer Records Act" ("CRA") was enacted to "encourage business that own, license, or maintain personal information about Californians to provide reasonable security for that information." Cal. Civ. Code § 1798.81.5(a)(1).

65. Under Section 1798.81.5(b), any business that "owns, licenses, or maintains personal information about a California resident" is required to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information," and "to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

66. Defendant was and still is a "business" under the terms of the CRA as a corporation operating in the State of California that collected personal information of Plaintiff and Class Members. Further, Defendant satisfies at least one of the requirements of Section 1798.140(c), as it "receives for the business' commercial purposes … or shares for commercial purposes… the personal information of 50,000 or more consumers, households, or devices."

67. Section 1798.81.5(d)(1)(B) defines "personal information" as including an individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted. This includes, but is not limited to, an individual's social security number; driver's license number; California identification card number; medical information, such as an individual's medical history or medical treatment or diagnosis by a health care professional; health insurance information,

such as individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals record; and more. *See* Cal. Civ. Code § 1798.81.5(d)(1)(A)-(B).

68. At all relevant times, Plaintiff and the California subclass were "customers" under the terms of the CRA as natural persons who provided personal information to Defendant for the purpose of obtaining a medical services or equipment from Defendant.

69. As alleged in detail above, Defendant failed to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information," and "to protect the personal information from unauthorized access, destruction, use, modification, or disclosure," resulting in the Data Breach.

70. Further, under Cal. Civ. Code § 1798.2, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

71. Under Cal. Civ. Code § 1798.2(b), the disclosure must "be made in the most expedient time possible and without unreasonable delay" but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

72. Here, Defendant possessed highly sensitive PII of Plaintiff and the Class Members in an unencrypted format, resulting in an unauthorized person acquired the personal, unencrypted information of Plaintiff and Class Members. Moreover, the personal information involved — such as names, addresses, dates of birth, social security numbers, and driver's license numbers — are not exempted from coverage by this statute due to the CMIA or HIPAA because it is not medical information.

73. Defendant knew that an unauthorized activity had potentially compromised personal, unencrypted information of Plaintiff and Class Members in July 2021, but waited until March 2022 to notify individuals of the breach. This eight month of delay was unreasonable under the circumstances.

74. Moreover, Defendant's unreasonable delay prevented Plaintiff and Class Members from taking appropriate measures from protecting themselves against harm by protecting their information or monitoring their data earlier. Because Plaintiff and Class Members were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

75. As such, Plaintiff and Class Members are entitled to equitable relief and damages in an amount to be determined at trial.

THIRD CAUSE OF ACTION

NEGLIGENCE

(on behalf of Plaintiff and the Nationwide Class)

76. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

77. Plaintiff and the Nationwide Class entrusted their PII and PHI to Defendant. Defendant owed to Plaintiff and the Nationwide Class a duty to exercise reasonable care in handling and using the PII and PHI in its care and custody. This includes including industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass; detecting attempts at unauthorized access; and promptly notifying those affected of potential harm.

78. Defendant owed a duty of care to Plaintiff and the Nationwide Class because it was foreseeable that Defendant's failure to adequately safeguard their PII and PHI in accordance with state-of-the-art industry standards concerning data security could result in the compromise of that PII and PHI.

79. Defendant was negligent in its handling of Plaintiff and the Nationwide

Class's PII and PHI by (1) disclosing and providing access to this information to third parties and (2) by failing to properly supervise both the way the information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

80. Further, Defendant owed Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII and PHI. Defendant also owed a duty to timely and accurately disclose the scope, nature, and occurrence of the Data Breach, in order for Plaintiff and Class Members to take appropriate measures to protect their information and mitigate the harm caused by the Data Breach.

81. Specifcally, under the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, Defendant was required to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach." Defendant failed to provide any notice to Plaintiff and Class Members until nearly *eight* months after becoming aware of unauthorized activity.

82. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff' and Class Member's PII and PHI.

83. The risk that unauthorized persons would attempt to gain access to the PII and PHI and misuse it was foreseeable. Given that Defendant holds vast amounts of PII and PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing this highly sensitive information.

84. PII and PHI are highly valuable—they can be sold on the black market and utilized in order to open fraudulent accounts or medical claims. Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing

Plaintiff and Class Members PII and PHI and the importance of exercising reasonable care in handling it.

85. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII and PHI of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, and emotional distress.

86. Neither Plaintiff nor the other Class Members contributed to the unauthorized data breach as described in this Complaint.

87. As a direct and proximate cause of Defendant's conduct, Plaintiff and class members have suffered and/or will suffer injury and damages, including but not limited to: (a) the loss of the opportunity to determine for themselves how their PII and PHI is used; (b) the publication and/or potential theft of their PII and PHI; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the unauthorized data breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from fraud and identity theft; (e) costs associated with placing freezes on credit reports beyond the free credit monitoring provided by Defendant; (f) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (g) the continued risk to their PII, which remains in Defendant's possession (and/or

Defendant has access to) and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession; and, (h) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII and PHI.

88. As a direct and proximate result of Defendant's negligence, Plaintiff and class members have been injured as described herein, and are entitled to damages including, but not limited to, compensatory, nominal, and consequential damages.

FOURTH CAUSE OF ACTION

NEGLIGENCE PER SE

(on behalf of Plaintiff and the Nationwide Class)

89. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

90. Pursuant to the Federal Trade Commission ("FTC") Act of 1914, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Member's PII and PHI.

91. In 2016, the FTC established guidelines for fundamental data security principles and practices for business.[13] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of the breach.

92. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting

[13] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited May 12, 2022).

commerce," including, as interpreted andenforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' PII and PHI. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and Class Member's sensitive PII and PHI.

93. Here, Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its patients' PII and PHI and not complying with applicable industry standards. Moreover, Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its patientsin the event of a breach, which ultimately came to pass.

94. Plaintiff and the Class Members are among the class of persons Section 5 of the FTC was designed to protect, and the injuries suffered by Plaintiff and the class members are the types of injury Section 5 of the FTC Act was intended to prevent. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class Members.

95. Defendant had a duty to Plaintiff and Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Member's PII and PHI.

96. Defendant breached its respective duties to Plaintiff's and Class Members' PII and PHI under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class Members' PII and PHI.

97. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

98. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Member, Plaintiff and Class Members would not have been injured.

99. As a direct and proximate cause of Defendant's conduct, Plaintiff and class members have suffered and/or will suffer injury and damages, including but not limited to: (a) the loss of the opportunity to determine for themselves how their PII and PHI is used; (b) the publication and/or theft of their PII and PHI; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the unauthorized data breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from fraud and identity theft; (e) costs associated with placing freezes on credit reports; (f) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (g) the continued risk to their PII, which remains in Defendant's possession (and/or Defendant has access to) and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession; and, (h) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII and PHI.

100. As a direct and proximate result of Defendant's negligence, Plaintiff and class members have been injured as described herein, and are entitled to damages including, but not limited to, compensatory, nominal, and consequential damages.

FIFTH CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

(on behalf of Plaintiff and the Nationwide Class)

101. Plaintiff hereby re-alleges and incorporates by reference the above

allegations by reference as if fully set forth herein.

102. Defendant exchanged medical equipment and services in exchange for their Plaintiff and Class Members' PII and PHI.

103. In turn, and through its own internal policies, Defendant agreed it would not disclose the PII and PHI it collects to unauthorized persons. Defendant also promised to safeguard patient PII and PHI.

104. Plaintiff and Class Members accepted Defendant's offer by providing PII and PHI to Defendant in exchange for Defendant's goods and services.

105. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII and PHI. Given the strict standards in place for the maintenance of health information, Plaintiff and Class Members believed that their highly sensitive information would be safeguarded in Defendant's control.

106. Defendant materially breached the contract(s) it had entered with Plaintiff and Class Members by failing to safeguard such information, as well as by failing to notify Plaintiff and Class Members promptly of the intrusion into its computer systems that compromised such information.

107. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

108. Plaintiff and Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

109. Defendant failed to advise Plaintiff and Class Members of the Data Breach promptly and sufficiently.

110. In these and other ways, Defendant violated its duty of good faith and fair dealing.

111. Plaintiff and Class Members have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations

of the covenant of good faith and fair dealing.

SIXTH CAUSE OF ACTION

INVASION OF PRIVACY

(on behalf of Plaintiff and the Nationwide Class)

112. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

113. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

114. Defendant owed a duty to its current and former patients, including Plaintiff and the Nationwide Class, to keep their PII and PHI contained as a part thereof, confidential.

115. Defendant failed to protect and actually or potentially released to unknown and unauthorized third parties the PII and PHI of Plaintiff and the Nationwide Class.

116. Defendant allowed unauthorized and unknown third parties to actually or potentially access and examineof the PII and PHI of Plaintiff and the Nationwide Class, by way of Defendant's failure to protect the PII and PHI.

117. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and PHIof Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

SEVENTH CAUSE OF ACTION

VIOLATION OF CALIFORNIA UNFAIR COMPETION LAW

(Cal. Bus. Code § 17200, *et seq*.)

(on behalf of Plaintiff and the California Class)

118. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

119. Defendant engaged in unlawful and unfair business practices in

violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

120. Defendant's conduct is unlawful because it violates Cal. Civ. Code § 56.10 *et seq,* by failing to maintain a proper electronic health record system or electronic medical record system that could "[p]rotect and preserve the integrity of electronic medical information," resulting in the disclosure of Plaintiff and the Class Member's PII and PHI.

121. Defendant's conduct is unlawful because it violates California Civil Code § 1798.80 by failing to employ reasonable security measures, resulting in an "unauthorized access, destruction, use, modification, or disclosure" of Plaintiff and Class Members' PII.

122. Defendant's conduct is unlawful because it violates section 5 of the FTC Act, by failing to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Member's PII and PHI, resulting in the Data Breach at issue.

123. Defendant stored the PII and PHI of Plaintiff and Class Members in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff and Class Members' PII and PHI secure and prevented the loss or misuse of that highly sensitive information.

124. Defendant failed to disclose to Plaintiff and Class Members that their PII and PHI was not secure. However, Plaintiff and Class Members were entitled to assume, and did assume, that Defendant had secured their PII and PHI. At no time were Plaintiff and Class Members on notice that their PII and PHI was not secure, which Defendant had a duty to disclose.

125. Had Defendant complied with these requirements, Plaintiff and Class Members would not have suffered the damages related to the data breach.

126. Further, Defendant's conduct was unlawful, in that it violated the

Consumer Records Act. Defendant made the PII and PHI of Plaintiff and Class Members accessible to scammers, identity thieves, and other malicious actors, subjecting these individuals to an impending risk of identity theft.

127. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

128. As a result of those unlawful and unfair business practices, Plaintiff and Class Members suffered an injury-in-fact and have lost money or property that cannot be recovered.

129. The injuries to Plaintiff and Class Members greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

130. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

131. Therefore, Plaintiff and Class Members are entitled to equitable relief including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

132. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII and PHI to Defendant as part of Plaintiff and Class Members' relationship with Defendant, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

133. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as totheir private affairs or concerns, of a kind that would

be highly offensive to a reasonable person.

134. Defendant acted knowingly and intentionally when it permitted the Data Breach to occur because it was with actual knowledge that its information security system and storage practices were inadequate and insufficient in light of the heavily sensitive information that it possessed.

135. As such, Defendant had sufficient notice that its inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class Members.

136. As a proximate result of the above acts and omissions of Defendant, the PII and PHI of Plaintiff and Class Members was accessed by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

137. Here, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries, as a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for judgment against Defendant as follows:

1. For certification of this action as a class action,
2. For appointment of Harmon Cottrell as the class representative;
3. For appointment of Lebe Law, APLC as class counsel for all purposes;
4. For compensatory damages in an amount according to proof with interest thereon;
5. For economic and/or special damages in an amount according to proof with interest thereon;
6. For pre-judgment interest; and

7. For other relief as the Court deems just and proper.

Dated: May 18, 2022

LEBE LAW, APLC

By: /s/ Jonathan M. Lebe
Jonathan M. Lebe
Zachary T. Gershman
Shigufa K. Saleheen
Attorneys for Plaintiff Harmon Cottrell

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial with respect to all issues triable of right by jury.

Dated: May 18, 2022

LEBE LAW, APLC

By: /s/ Jonathan M. Lebe
Jonathan M. Lebe
Zachary T. Gershman
Shigufa K. Saleheen
Attorneys for Plaintiff Harmon Cottrell

ClassAction.org
