Scott Edward Cole, Esq. (S.B. #160744)
Laura Grace Van Note, Esq. (S.B. #310160)
SCOTT COLE & ASSOCIATES, APC
555 12th Street, Suite 1725
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: scole@scalaw.com
Email: lvannote@scalaw.com
Web: www.scalaw.com

Attorneys for Representative Plaintiffs
and the Plaintiff Classes

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

MICHAEL RUBENSTEIN, RICHARD MACHADO, individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

SCRIPPS HEALTH,

Defendant.

Case No. **'21CV1135 DMS RBB**

CLASS ACTION

COMPLAINT FOR DAMAGES, RESTITUTION AND INJUNCTIVE/EQUITABLE RELIEF

JURY TRIAL DEMANDED

Representative Plaintiffs allege as follows:

INTRODUCTION

1. This is a class action brought by Representative Plaintiffs on behalf of themselves as well as on behalf of California and National classes of all entities/persons whose personally identifiable information was acquired, starting as early as April 29, 2021, by unauthorized persons in the data breach announced by Scripps Health ("Defendant") on or about June 1, 2021.

2. Representative Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard Representative Plaintiffs' and Class Members' personally

identifiable information stored within Defendant's information network, including, without limitation, their names, dates of birth, Social Security numbers and/or driver license numbers (these types of information, *inter alia*, being hereafter referred to, collectively, as "personally identifiable information" or "PII")[1] and to properly secure and safeguard Representative Plaintiffs' and Class Members' personal health information stored within Defendant's information network, including, without limitation, their health insurance information, medical record numbers, patient account numbers, and/or clinical information such as physician(s) name, date(s) of service, doctor progress notes, lab test results, and/or treatment information (these types of information, *inter alia*, being hereafter referred to, collectively, as "personal health information" or "PHI")[2]

3. As San Diego, California's second largest healthcare provider, Defendant acquired, collected and stored Representative Plaintiffs' and Class Members' PII/PHI in order to ensure efficient and quality healthcare to its patients. Therefore, at all relevant times, Defendant knew or should have known that its patients would use Scripps Health to store and/or share sensitive data, including highly confidential PII/PHI, because Defendant promised them that creating personal healthcare records would improve health care quality.

4. At a minimum, at least according to Defendant's admissions, the compromised files and data contained the PII/PHI of Representative Plaintiffs and Class Members, including, but not necessarily limited to, names, dates of birth, Social Security numbers and/or driver license numbers, health insurance information, medical record numbers, patient account numbers, and/or clinical information such as physician(s) name, date(s) of service, doctor progress notes, lab test results, and/or treatment information.

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[2] Personal health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act (HIPAA). Inter alia, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

5. The HIPAA Privacy Rule (45 CFR, Parts 160 and 164(A) and (E), among other sections, hereinafter "HIPAA") establishes national minimum standards for the protection of individuals' medical records and other personal health information. HIPAA, generally, applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, and sets minimum standards for Defendant's maintenance of Representative Plaintiffs' and Class Members' personal and medical information. More specifically, HIPAA requires appropriate safeguards be maintained by healthcare providers such as Defendant to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. HIPAA also establishes a series of patients' rights over their health information, including rights to examine and obtain copies of their health records, and to request corrections thereto.

6. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

7. By obtaining, collecting, using, and deriving a benefit from Representative Plaintiffs' and Class Members' PII/PHI, Defendant assumed legal and equitable duties to those individuals.

8. The exposed PII/PHI of Representative Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII/PHI to criminals. Given Defendant's misconduct in allowing hackers to access such information in this instance, Representative Plaintiffs and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

9. This PII/PHI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect PII/PHI of Representative Plaintiffs and Class Members.

10. Representative Plaintiffs bring this action on behalf of all persons whose PII/PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII/PHI of

Representative Plaintiffs and Class Members; (ii) warn Representative Plaintiffs and Class Members of these inadequate information security practices; and (iii) effectively secure hardware containing protected PII/PHI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

11. Representative Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII/PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued increased risk to their PII/PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI.

12. Defendant disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' PII/PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII/PHI of Representative Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Representative Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

JURISDICTION AND VENUE

13. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction) and/or 28 U.S.C. §1331 (controversy arising under United States law). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member is a citizen of a state different from Defendant.

14. Supplemental jurisdiction to adjudicate issues pertaining to California state law is proper in this Court under 28 U.S.C. §1367.

15. Defendant routinely conducts business in California, has sufficient minimum contacts in California and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within California.

16. Venue is proper in this Court under 28 U.S.C. § 1391 because the events that gave rise to Representative Plaintiffs' claims took place within the Southern District of California, and Defendant does business in this Judicial District.

PLAINTIFFS

17. Representative Plaintiff Michael Rubenstein is an adult individual and resident of the State of California. He is referred to in this Complaint simply as "Rubenstein" or, collectively with his fellow plaintiff, as a "Representative Plaintiff." Rubenstein is a victim of the Data Breach.

18. At all times herein relevant, Rubenstein is and was a member of the National class and the California Subclass.

19. Rubenstein's PII/PHI was exposed in the Data Breach because Scripps Health stored and/or shared Rubenstein's PII/PHI. In late April 2021, an unauthorized person gained access to Defendant's network, deployed malware, and, on April 29, 2021, acquired copies of numerous documents/records within Defendant's system. The PII/PHI included both personal and health information of Rubenstein and Class Members.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

20. On or around April 30, 2021, Rubenstein learned of the Data Breach. Initially, he tried to log onto Defendant's online patient portal and Epic Electronic Medical Record ("EMR") system and found it nonfunctional and inaccessible. Rubenstein manages a chronic health condition, as further detailed below and, because of this, uses Defendant's online patient portal and Epic Electronic Medical Record system nearly every day to manage his care. When Rubenstein discovered these systems were inaccessible, he investigated by calling several of his Scripps Health doctors' offices; eventually, he was able to gain some information from a nurse on or around May 1, 2021, who told him there had been a "cyber-attack" on Defendant's online network. Rubenstein then began conducting research online and via various news sources, at which point he discovered more specific details about the Data Breach.

21. As Rubenstein began to glean details of the Data Breach, he telephoned the administration line of Defendant's Chief Executive Officer ("CEO"). Despite multiple telephone calls of this nature during the first week of May 2021, including leaving several voicemail messages, no one ever called him back.

22. Rubenstein has been diagnosed with Primary Polycythemia (or polycythemia vera), also called Myelofibrosis due to his progressed condition. This blood disorder results in Rubenstein having a higher red blood cell count than the average person. While this condition is incurable, many of the condition's effects can be managed through medication. Rubenstein is currently disabled and collects disability through social security, his previous employer and his own medical coverage. Due to Rubenstein's chronic condition, he manages his healthcare through Defendant's patient portal and Epic EMR.

23. Because of Rubenstein's condition, he must constantly monitor his disease state through the lab results accessible through Defendant's patient portal and Epic EMR in order to determine the proper administration of his ongoing prescribed medications. However, as a result of the Data Breach, both the past lab results and future lab orders that Rubenstein had through July 2021 were inaccessible to him. Additionally, there were no alternative or backup systems in place for Rubenstein to access his laboratory information since all of Defendant's lab results and lab orders are electronically stored and accessible.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

24. During the system outage caused by the Data Breach, Rubenstein attempted to call his doctors but did not receive any answers or responses to his voicemails. Rubenstein then visited, in person, his hematologist's office, but his doctors were unavailable. Finally, Rubenstein was forced to visit a Scripps Health hematology clinic and beg a nurse to provide for him his lab orders.

25. As a result, as of May 2021, Rubenstein's only option was to take his medication without specific knowledge of his laboratory results. This was potentially dangerous to Rubenstein as he was unable to confirm whether the timing/administration of particular dosages was correct.

26. Additionally, Rubenstein attempted to receive medical advice from hematologists outside of Defendant's healthcare system. Rubenstein was unsuccessful in these efforts insofar as these independent hematologists would not see him without the notes from a prior hematologist—notes that were inaccessible to Rubenstein as a result of the Data Breach—or would have to re-diagnose all or portions of Rubenstein's condition through procedures that would have been time consuming and invasive.

27. Furthermore, Rubenstein altogether missed a regularly scheduled bone marrow biopsy in May 2021 due to the Data Breach and its resultant online network failure. Rubenstein receives a bone marrow biopsy every four to five years in order to accurately assess his current health condition. Reviewing the results of these biopsies is critical for his doctors to determine and advise in favor or against different treatment options. Similar to his reactions to the other events described above, Rubenstein experienced emotional distress in the form of anxiety and lost sleep due to missing this critical appointment.

28. Representative Plaintiff Richard Machado is an adult individual and resident of the State of California. He is referred to in this Complaint simply as "Machado" or, collectively with his fellow plaintiff, as a "Representative Plaintiff." Machado is a victim of the Data Breach.

29. At all times herein relevant, Machado is and was a member of the National class and the California Subclass.

30. Machado's PII/PHI was exposed in the Data Breach because Defendant Scripps Health stores and/or shared Machado's PII/PHI. In late April 2021, an unauthorized person gained access to Defendant's network, deployed malware, and, on April 29, 2021, acquired copies of

some of the documents on Defendant's system. The PII/PHI included both personal and health information of Machado and numerous other Class Members.

31. On or around June 1, 2021, Machado learned of the Data Breach. Because Machado was no longer an active patient of Scripps Health at the time of the Data Breach, he was not aware that Defendant's patient portal was inoperable or that the Data Breach had occurred until he received a letter in the mail from Defendant that, at least summarily, described the unauthorized access of the Scripps Health network and the information that was compromised. Again, this was more than a month after Defendant's network was unlawfully accessed.

32. Machado was diagnosed with Type 2 Diabetes while a patient of Scripps Health several years ago. As a further result of his condition, Machado underwent a very personal surgery that was extremely painful and private for him. Records exist within Scripps Health's data network and/or ancillary systems regarding these procedures and are highly personal to Machado.

33. Machado was aware that Scripps Health still had his personal medical history and diagnoses on file in its Epic Electronic Medical Record and/or ancillary systems, and he trusted Defendant to safeguard his private information.

34. Machado underwent extensive treatment for his Type 2 Diabetes while a patient of Scripps Health, so his potential private information compromised is vast.

35. It was not until June 1, 2021 that each of the Representative Plaintiffs received a letter in the mail that described (at least summarily) the unauthorized access of the Scripps Health network and the information that was compromised.

36. As a result of the Data Breach, each of the Representative Plaintiffs spent time dealing with the consequences of the Data Breach, which included time spent attempting to contact Scripps Health representatives, exploring alternative healthcare options, verifying the legitimacy of the news reports about the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring their accounts and/or researching and contacting professionals, including legal counsel. This time has been lost forever and cannot be recaptured.

37. Additionally, Representative Plaintiffs are very careful about sharing their PII/PHI, particularly details of their medical diagnoses and healthcare treatment plans. Their privacy is of

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

utmost importance to them, and Defendant breached its duty of care regarding this privacy. Representative Plaintiffs have never knowingly transmitted unencrypted PII/PHI over the internet or any other unsecured source, and never share information about their healthcare with anyone who does not need to know about it.

38. Representative Plaintiffs further suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, were, in some instances, unable to access their EMR/EHR via the Scripts online portal (resulting in short and/or long term health risks) and/or have anxiety and increased concerns for the loss of their privacy and the inability for Defendant to safeguard their PII/PHI and other health information, as well as to have a competent backup system in place in the case of an attack like the one that resulted in this Data Breach.

39. Representative Plaintiffs have a continuing interest in ensuring that their PII/PHI and health information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

40. Representative Plaintiffs bring this action on behalf of themselves, and as a class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of all persons similarly situated and proximately damaged by the unlawful conduct described herein.

DEFENDANT

41. Defendant Scripps Health is a California corporation with its principal place of business located at 10140 Campus Point Drive, San Diego, California 92121.

42. Originally founded in 1924 by Ellen Browning Scripps as a philanthropic project, Defendant's private, nonprofit health system now includes four hospitals on five campuses along with 28 outpatient facilities and clinics.[3] Defendant treats 700,000 patients annually through more than 3,000 affiliated physicians and offers clinical research and medical education programs, presented by well over 15,000 employees and volunteers.[4]

[3] https://www.scripps.org/about-us/who-we-are.
[4] *Id.*

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

43. Defendant's failure to protect Representative Plaintiffs and Class Members' data was not for lack of resources. In its fiscal year ending in September 2019, Defendant reported total revenue of $3,345,481,577 and net revenue less expenses of $274,752,677, with $113,859,866 in investment income alone.[5] In that same fiscal year, Defendant reported net assets of 4,250,272,456.[6]

44. What's more, the scope and sophistication of Defendant's operation is further reflected in the large salaries of its executives. In fiscal year ending in September 2019, Defendant paid President Christopher Van Gorder over $1.9 million, down from a staggering $8.6 million it paid him the prior year.[7] Other executives also take home seven figure annual compensation packages and several other employees earn in the high six figures.[8]

45. Despite its impressive profitability and lavish executive compensation, Defendant pitches itself as an organization primarily committed to the public good. On its website, Defendant bills itself as "San Diego's trusted leader for quality healthcare." Defendant claims it seeks to carry out the vision of its founders by dedicating itself to "quality, safe, cost-efficient, socially responsible health care for everyone we serve." Defendant purports to be more than a mere healthcare provider, but "a partner who believes in the healthiest version of you." Defendant's failure to safeguard Representative Plaintiffs' and Class Members' highly sensitive data, despite having adequate resources to do so, belies this high-minded sentiment.

46. In addition to violating its purported commitment to its patients and community, Defendant's failure to adequately secure Representative Plaintiffs' and Class Members' sensitive data also breaches duties it owes Representative Plaintiffs and Class Members under statutory and common law. Under the Health Insurance Portability Act of 1996, healthcare providers have an affirmative duty to keep patients' Protected Health Information private. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard

---

[5] 2018 990 Form available at https://projects.propublica.org/nonprofits/organizations/951684089.
[6] *Id.*
[7] 2017 990 Form available at https://projects.propublica.org/nonprofits/organizations/951684089.
[8] *Id.*

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Representative Plaintiffs' and Class Members' data. Moreover, Representative Plaintiffs and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data independent of any statute.

47. Defendant violated its duty to Representative Plaintiffs and Class Members through its failure to protect against a foreseeable cyberattack–a perhaps unsurprising fact given that Scripps Health failed to satisfy its own "mission" of devoting its "resources to delivering quality, safe, cost effective, socially responsible health care services."

48. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's, treatment plans) that is valuable to cyber criminals. One patient's complete record can be sold for hundreds of dollars on the dark web.[9] Unsurprisingly, thus, the healthcare industry is at high risk and acutely affected by cyber-attacks.[10]

49. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.[11] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[12] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03% of overall health data breaches, according to cybersecurity firm Tenable.[13]

50. Health data breaches are particularly concerning because they can lead not only to the disclosure of sensitive data, but to substandard treatment and negative health outcomes.[14] The devastating consequences of network interruption for patients is what makes health systems so tempting a target for attacks in the first place. Cybercriminals view patient care facilities as being

[9] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B4-healthcare-08-00133 (citing Chernyshev, M., Zeadally, S. & Baig, Z. Healthcare Data Breaches: Implications for Digital Forensic Readiness. J Med Syst 43, 7 (2019).
[10] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4479128/.
[11] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133.
[12] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.
[13] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.
[14] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B8-healthcare-08-00133.

more likely to pay ransoms to restore access to their systems since extended downtime is intolerable.[15] Indeed, as Representative Plaintiff Rubenstein experienced here, losing access to the system can have serious adverse consequences for patient health. Consequently, health data systems require enhanced security and should be breach-proof.[16] Because hacking attacks using malware or ransomware represent a significant portion of all data breaches or unlawful disclosures, healthcare providers should be prepared for such attacks. As such, Defendant's failure to protect against the attack was negligent and or reckless in violation of its legal duty to Representative Plaintiffs and Class Members.

51. 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 here are currently unknown to Representative Plaintiffs. Representative Plaintiffs 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.

CLASS ACTION ALLEGATIONS

52. Representative Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the following classes/subclass(es) (collectively, the "Classes"):

California class:
"All individuals within the State of California whose PII/PHI was stored by Defendant and/or was exposed to unauthorized third parties as a result of the compromise of Scripps Health's data systems, as announced on or about June 1, 2021."

National class:
"All individuals within the United States of America whose PII/PHI was stored by Defendant and/or was exposed to unauthorized third parties as a result of the compromise of Scripps Health's data systems, as announced on or about June 1, 2021."

53. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which

[15] https://www.cpomagazine.com/cyber-security/rise-in-healthcare-data-breaches-driven-by-ransomware-attacks/.
[16] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B8-healthcare-08-00133.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

54. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed classes is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiffs are informed and believe and, on that basis, allege that the total number of Class Members is in the hundreds of thousands of individuals. Membership in the classes will be determined by analysis of Defendant's records.

b. Commonality: The Representative Plaintiffs and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendant had a legal duty to Representative Plaintiffs and the Classes to exercise due care in collecting, storing, using and/or safeguarding their PII/PHI;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

6) Whether Defendant adequately, promptly, and accurately informed Representative Plaintiffs and Class Members that their PII/PHI had been compromised;

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII/PHI of Representative Plaintiffs and Class Members;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Representative Plaintiffs and Class Members;

11) Whether Representative Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

12) Whether Representative Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: The Representative Plaintiffs' claims are typical of the claims of the Plaintiff Classes. Representative Plaintiffs and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: The Representative Plaintiffs in this class action are adequate representatives of each of the Plaintiff Classes in that the Representative Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. The Representative Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in their entirety. The Representative Plaintiffs anticipate no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Plaintiff classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

55. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's

imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes in their entireties. Defendant's policies challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Classes in their entireties, not on facts or law applicable only to the Representative Plaintiffs.

56. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII/PHI of Class Members, Defendant may continue to act unlawfully as set forth in this Complaint.

57. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COMMON FACTUAL ALLEGATIONS

Defendant's Unlawful Conduct

58. On May 1, 2021, Scripps Health identified unusual network activity and initiated its response protocols with the assistance of computer forensic firms. The investigation determined that an unauthorized person gained access to the network, deployed malware, and acquired copies of many of the documents on Defendant's system as early as April 29, 2021.

59. As a result of the attack, Defendant's IT systems were suspended, including public-facing portals such as EPIC, MyScripps and scripps.org. It was not until one month after this outage began that the electronic health records were back online and functioning, allowing patients to log into their MyScripps accounts and schedule appointments online. During the outage, hospitals in Encitas, La Jolla, San Diego and Chula Vista no longer received certain patients such as stroke or heart attack victims. Instead, those persons in need were diverted to other medical facilities because of the backlog of requests.

60. In addition to the patients harmed by the outage, many Scripps Health business support workers were unsure if and when they would receive their paychecks while the systems

remained offline. As a result, many or all of them were instructed to either use their paid time off or work without pay during the month of May 2021, a blatant violation of California wage and hour laws.

61. On May 10, 2021, after review of the unauthorized acquired documents, it was discovered that the seized documents contained patient information including names, dates of birth, Social Security numbers and/or driver license numbers, health insurance information, medical record numbers, patient account numbers, and/or clinical information such as physician(s) names, date(s) of service, doctor progress notes, lab test results, and/or other treatment information.

62. More than 147,000 patients, staff and physicians have had their personal and financial information compromised by this cyberattack on Scripps Health's internal systems. For those patients whose data was exposed, Scripps Health mailed notification letters on June 1, 2021. The letter informed patients of the Data Breach and Defendant's recommended next steps such as reviewing statements received from healthcare providers and insurers.

63. The letter also informed patients whose Social Security or driver's license numbers were thought exposed during the attack that they would be offered a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product is marketed as helping to detect possible misuse of personal information and to provide users with identity protection support focused on immediate identification and resolution of identity theft.

64. This complimentary service, however, does not and will not fully protect the patients from cyber criminals and is largely ineffective against protecting data after it has been stolen. Cyber criminals are fully aware of the well-publicized preventative measures taken by entities after data breaches such as that which happened here and will, therefore, oftentimes hold onto the stolen data and not use it until after the complimentary service is no longer active, and long after victim concerns and preventative steps have diminished. Consistent with these realities, Scripps Health' offer to provide a complimentary one-year membership of Experian IdentityWorksSM Credit 3B will likely prove largely ineffectual in combating the misuse of Representative Plaintiffs' and Class Members' PII/PHI.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

65. Scripps Health has described that performing an extensive review of the stolen documents is a time intensive process and that it will likely take several months to fully inventory the information and documents accessed in the Data Breach. As of the date of filing of this Complaint, the investigation into the cyber-attack is ongoing.

66. In its announcement, Defendant alleged it learned of "unusual network activity" as early as May 1, 2021. Despite this knowledge, Defendant failed to notify Representative Plaintiffs and Class Members of the Data Breach until June 1, 2021.

67. The announcement included the following:

> On May 1, 2021, we identified unusual network activity. We immediately initiated our incident response protocols, which included isolating potentially impacted devices and shutting off select systems. We also began an investigation with the assistance of computer forensic firms. The investigation determined that an unauthorized person gained access to our network, deployed malware, and, on April 29, 2021, acquired copies of some of the documents on our system. On May 10, 2021, we discovered that some of those documents contained patient information. Upon conducting a review of those documents, we determined that one or more files may have reflected your name, address, date of birth, health insurance information, medical record number, patient account number, and/or clinical information, such as physician name, date(s) of service, and/or treatment information.
>
> We have no indication that any of your information has been used to commit fraud. However, we recommend that you review the statements you receive from your healthcare providers and health insurer. If you see any medical services that you did not receive, please call the provider or insurer immediately. To help prevent something like this from happening again, we are continuing to implement enhancements to our information security, systems, and monitoring capabilities.[17]

68. Despite this notification, Representative Plaintiffs and the Class Members remain, even today, in the dark regarding what data was stolen, the particular malware used, and what steps are being taken to secure their PII/PHI going forward. Indeed, even the particular "computer forensic firms" being employed is left a mystery, such that the quality of that forensic work is left in question. Especially in light of Defendant's suggestion that patients "review the statements [they] receive from [their] healthcare providers and health insurer[s]," Representative Plaintiffs and Class Members are left to speculate as to the full impact of the Data Breach and how exactly

[17] Scripps- Letter Sample.pdf (ca.gov) (last visited June 17, 2021).

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Defendant intends to "enhance" its information security, systems, and monitoring capabilities so as to prevent further breaches.

69. Thus far, Defendants have admitted that approximately 147,267 patients had their personal information accessed, with an alleged 2.5 percent, or 3,700, of those patients having had their Social Security and/or driver's license numbers taken.

70. As a result of the sensitive nature of the information it harvested and held, Defendant was well aware this PII/PHI presented a very attractive target for hackers, and yet, failed to take industry standard steps to protect the data.

71. Representative Plaintiffs' and Class Members' information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII/PHI for targeted marketing without the approval of Representative Plaintiffs and/or Class Members. Unauthorized individuals can easily access the PII/PHI of Representative Plaintiffs and Class Members.

72. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Representative Plaintiffs and Class Members, causing their PII/PHI to be exposed.

Defendant Maintained Representative Plaintiffs' and Class Members' PII/PHI

73. Defendant acquired, collected, and stored Representative Plaintiffs' and Class Members' PII/PHI.

74. At all relevant times, Defendant knew or should have known that its patients would use Scripps Health to store and/or share sensitive data, including highly confidential PII/PHI, because Defendant promised those patients that creating personal healthcare records would improve their health care quality.

75. Indeed, personal health records can improve patient engagement, coordinate and combine information from multiple healthcare providers, ensure availability of patient information online, reduce administrative costs and enhance provider-patient communication.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

76. By obtaining, collecting, and storing Representative Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Representative Plaintiffs' and Class Members' PII/PHI from unauthorized disclosure.

77. Representative Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PI PII/PHI I. Representative Plaintiffs and Class Members relied on Defendant to keep their PII/PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

78. Defendant could have prevented this Data Breach by properly securing and encrypting Representative Plaintiffs' and Class Members' PII/PHI.

79. Defendant's negligence in safeguarding Representative Plaintiffs' and Class Members' PII/PHI is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

80. The healthcare industry has experienced a large number of high-profile cyber-attacks even in just the one-year period preceding the filing of this Complaint and cyber-attacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[18] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported in April 2021.[19]

81. For example, one of Scripps Health's competitors, Universal Health Services, experienced a cyber-attack on September 29, 2020 that was very similar to the attack on Scripps Health. Not unlike Scripps Health, Universal Health Services suffered a four-week outage of its systems which caused as much as $67 million in recovery costs and lost revenue.[20] Due to the high-profile nature of the Universal Health Services breach, and other breaches of its kind, Scripps

[18] https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/ (last accessed June 17, 2021).
[19] https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/ (last accessed June 17, 2021).
[20] https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and (last accessed June 17, 2021).

Health was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack.

82. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' PII/PHI from being compromised.

Value of Personal Identifiable Information

83. Personal data such as that hacked in the Data Breach represents a major score for cybercriminals who will likely look to capitalize on it by launching targeted phishing campaigns.

84. Indeed, it is well known and the subject of many media reports that Personal Information is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, Defendant maintained an insufficient and inadequate system to protect the Personal Information of Representative Plaintiffs and Class Members.

85. Personal Information is a valuable commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. Personal Information is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

86. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[21] 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

[21] 17 C.F.R. § 248.201 (2013).

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

license or identification number, alien registration number, government passport number, employer or taxpayer identification number." [22]

87. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance." See, Federal Trade Commission, Warning Signs of Identity Theft, available at: https://www.identitytheft.gov/warning-signs-of-identity-theft (last visited June 17, 2021).

88. Identity thieves can use personal information, such as that of Representative Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

89. Legitimate organizations and the criminal underground alike recognize the value in Personal Information contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million patients, they also took registration data [containing Personal Information] from 38 million users." (See, Verizon 2014 PCI Compliance Report, available at: https://www.centurybizsolutions.net/wp-content/uploads/2014/09/PCI-Compliance-report-2014.pdf, at 54).

90. The ramifications of Defendant's failure to keep secure Representative Plaintiffs' and Class Members' PII/PHI are long lasting and severe. Once PII/PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

91. As such, the PII/PHI 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

[22] *Id.*

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.[23] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[24] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[25]

92. 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 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.[26]

93. 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.

94. 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

[23] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed June 18, 2021).

[24] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed June 18, 2021).

[25] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed June 18, 2021).

[26] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed June 17, 2021).

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[27]

95. 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.

96. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license numbers or government-issued identification numbers, names, and dates of birth.

97. 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."[28]

98. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

99. The PII/PHI of Representative Plaintiffs and Class Members was taken by hackers to engage in identity theft 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.

100. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII/PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [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.[29]

---

[27] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed June 18, 2021).

[28] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed June 18, 2021).

[29] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:*

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

101. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Representative Plaintiffs' and Class Members' PII/PHI, including social security numbers, driver's license or state identification numbers, and/or dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Representative Plaintiffs and Class Members as a result of a breach.

102. As a result of the Data Breach, the Personal Information of Representative Plaintiffs and Class Members has been exposed to criminals for misuse. The injuries suffered by Representative Plaintiffs and Class Members, or likely to be suffered thereby as a direct result of the Defendant's Data Breach, include:

a. unauthorized use of their Personal Information;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their Personal Information;

e. loss of privacy, and embarrassment;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals and already misused via the sale of Representative Plaintiffs' and Class Members' information on the Internet black market;

h. damages to and diminution in value of their Personal Information entrusted to Defendant for the sole purpose of purchasing products and services from Defendant; and the loss of Representative Plaintiffs' and Class Members' privacy.

103. The injuries to the Representative Plaintiffs and Class Members were directly and proximately cause by Defendant's failure to implement or maintain adequate data security measures for this Personal Information.

---

http://www.gao.gov/new.items/d07737.pdf (last accessed June 17, 2021).

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

104. The Data Breach was the inevitable result of Defendant's inadequate approach to data security and the protection of the Personal Information that it collected during the course of business and, as such, Defendant could have prevented this Data Breach. It had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

105. Had Defendant remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the Data Breach and, ultimately, the theft of its patients' Personal Information.

106. Representative Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any actual fraudulent usage of their PII/PHI.

107. The injuries to Representative Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII/PHI of Representative Plaintiffs and Class Members.

FIRST CLAIM FOR RELIEF
NEGLIGENCE
(Both Classes)

108. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

109. At all times herein relevant, Defendant owed Representative Plaintiffs and members of both classes a duty of care, *inter alia*, to act with reasonable care to secure and safeguard the Personal Information of Representative Plaintiffs and Class Members and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the Personal Information of Representative Plaintiffs and Class Members in its computer systems and on its networks.

110. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Personal Information in its possession;

b. to protect Personal Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches.

111. Defendant knew that the Personal Information was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Representative Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

112. Defendant knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its data security systems, and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

113. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Representative Plaintiffs' and/or Class Members' Personal Information.

114. Defendant breached its duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Personal Information of Representative Plaintiffs and Class Members.

115. Because Defendant knew that a breach of its systems would damage hundreds of thousands of individuals, including Representative Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the Personal Information contained thereon.

116. Representative Plaintiffs' and Class Members' willingness to entrust Defendant with their Personal Information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the Personal Information its stored on them from attack.

117. Defendant had a special relationship with Representative Plaintiffs and Class Members.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

118. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiffs' and Class Members' Personal Information and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Representative Plaintiffs and/or Class Members.

119. Defendant breached its general duty of care to Representative Plaintiffs and members of both Classes in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Personal Information of Representative Plaintiffs and Class Members;

b. by failing to timely and accurately disclose that Representative Plaintiffs' and Class Members' Personal Information had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard Personal Information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Personal Information;

d. by failing to provide adequate supervision and oversight of the Personal Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Personal Information of Representative Plaintiffs and Class Members, misuse the Personal Information and intentionally disclose it to others without consent.

120. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the Personal Information to Representative Plaintiffs and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information.

121. Defendant breached its duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting a month after learning of the breach to notify Representative Plaintiffs and Class Members and then by failing to provide Representative Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiffs and Class Members regarding the extent of the

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

unauthorized access and continues to breach its disclosure obligations to Representative Plaintiffs and Class Members.

122. Further, through its failure to provide timely and clear notification of the Data Breach to Representative Plaintiffs and Class Members, Defendant prevented Representative Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII/PHI, and to access their medical records and histories.

123. There is a close causal connection between Defendant's failure to implement security measures to protect the PII/PHI of Representative Plaintiffs and Class Members and the harm suffered or risk of imminent harm suffered by Representative Plaintiffs and Class Members. Representative Plaintiffs' and Class Members' PII/PHI was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII/PHI by adopting, implementing, and maintaining appropriate security measures.

124. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII/PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

125. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiffs and Class Members.

126. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

127. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII/PHI is used;(iii) the compromise, publication, and/or theft of their PII/PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or

unauthorized use of their PII/PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) lost continuity in relation to their healthcare; (vii) costs associated with placing freezes on credit reports; (viii) the continued risk to their PII/PHI, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' PII/PHI in its continued possession; and (ix) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members.

128. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

129. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII/PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI in its continued possession.

SECOND CLAIM FOR RELIEF
INVASION OF PRIVACY
(Both Classes)

130. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

131. Representative Plaintiffs and Class Members had a legitimate expectation of privacy to their PII/PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

132. Defendant owed a duty to Representative Plaintiffs and Class Members to keep their PII/PHI confidential.

133. Defendant failed to protect and released to unknown and unauthorized third parties the PII/PHI of Representative Plaintiffs and Class Members.

134. Defendant allowed unauthorized and unknown third parties access to and examination of the PII/PHI of Representative Plaintiffs and Class Members, by way of Defendant's failure to protect the PII/PHI.

135. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII/PHI of Representative Plaintiffs and Class Members is highly offensive to a reasonable person.

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

137. The Data Breach at the hands of Defendant constitutes an intentional interference with Representative Plaintiffs' and Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

138. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

139. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Representative Plaintiffs and Class Members.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

140. As a proximate result of the above acts and omissions of Defendant, the PII/PHI of Representative Plaintiffs and Class Members was disclosed to third parties without authorization, causing Representative Plaintiffs and Class Members to suffer damages.

141. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Representative Plaintiffs and Class Members in that the PII/PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Representative Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Representative Plaintiffs and/or Class Members.

THIRD CLAIM FOR RELIEF
CALIFORNIA CUSTOMER RECORDS ACT (CAL. CIV. CODE §1798.80, ET SEQ.)
(California Subclass Only)

142. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

143. Representative Plaintiffs bring this cause of action on behalf of the members of the California subclass whose personal information is maintained by Defendant and/or that was compromised in the Data Breach announced in June 2021.

144. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted California Customer Records Act. This statute states that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Civil Code § 1798.81.5.

145. Defendant is a "business" within the meaning of Civil Code § 1798.80(a).

146. Representative Plaintiffs and members of the California subclass are "individual[s]" within the meaning of the Civil Code § 1798.80(d). Pursuant to Civil Code §§ 1798.80(e) and 1798.81.5(d)(1)(C), "personal information" includes an individual's name, Social Security number, driver's license or state identification card number. "Personal information" under

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Civil Code §1798.80(e) also includes address, telephone number, passport number, education, employment, or employment history.

147. The breach of the personal data of well over one hundred thousand Defendant patients instituted a "breach of the security system" of Defendant pursuant to Civil Code §1798.82(g).

148. By failing to implement reasonable measures to protect its patients' personal data, Defendant violated Civil Code §1798.81.5.

149. In addition, by failing to promptly notify all affected patients that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the Data Breach, Defendant violated Civil Code § 1798.82 of the same title. Defendant's failure to timely notify its patients of the breach has caused damage to California Class Members who have had to buy identity protection services or take other measures to remediate the breach caused by Defendant's negligence.

150. By violating Civil Code §§1798.81.5 and 1798.82, Defendant "may be enjoined" under Civil Code §1798.84(e).

151. Accordingly, Representative Plaintiffs requests that the Court enter an injunction requiring Defendant to implement and maintain reasonable security procedures to protect patients' data in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis; (2) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and securing checks; (5) ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

identify and contain a breach when it occurs and what to do in response to a breach; and (6) ordering Defendant to adequately encrypt sensitive personal information.

152. Representative Plaintiffs further request that the Court require Defendant to (1) identify and notify all members of the California subclass who have not yet been informed of the Data Breach; and (2) to notify affected former and current patients of any future data breaches by email within 24 hours of Defendant's discovery of a breach or possible breach and by mail within 72 hours.

153. As a result of Defendant's violation of Civil Code §§ 1798.81.5, and 1798.82, Representative Plaintiffs and members of the California subclass have and will incur economic damages relating to time and money spent remedying the breach, including but not limited to, expenses for bank fees associated with the breach, any unauthorized charges made on financial accounts, identity and tax fraud, as well as the costs of credit monitoring and purchasing credit reports, and damages associated with loss of continuity of their health care.

154. Representative Plaintiffs, individually and on behalf of the members of the California subclass, seek all remedies available under Civil Code §1798.84, including, but not limited to: (a) damages suffered by members of the California Subclass; and (b) equitable relief.

FOURTH CLAIM FOR RELIEF
UNFAIR BUSINESS PRACTICES (CAL. BUS. & PROF. CODE, §17200, ET SEQ.)
(California Subclass Only)

155. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

156. Representative Plaintiffs and members of the California subclass further bring this cause of action, seeking equitable and statutory relief to stop the misconduct of Defendant, as complained of herein.

157. The knowing conduct of Defendant, as alleged herein, constitutes an unlawful and/or fraudulent business practice, as set forth in California Business & Professions Code §§17200-17208. Specifically, Defendant conducted business activities while failing to comply

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

with the legal mandates cited herein, including HIPAA. Such violations include, but are not necessarily limited to:

a. failure to maintain adequate computer systems and data security practices to safeguard Personal Information;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard Personal Information from theft;

c. failure to timely and accurately disclose the Data Breach to Representative Plaintiffs and members of the California subclass;

d. continued acceptance of Personal Information and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. continued acceptance of Personal Information and storage of other personal information after Defendant knew or should have known of the Data Breach and before it allegedly remediated the Breach.

158. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Personal Information of Representative Plaintiffs and members of the California subclass, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

159. In engaging in these unlawful business practices, Defendant has enjoyed an advantage over its competition and a resultant disadvantage to the public and members of the California subclass.

160. Defendant's knowing failure to adopt policies in accordance with and/or adhere to these laws, all of which are binding upon and burdensome to Defendant's competitors, engenders an unfair competitive advantage for Defendant, thereby constituting an unfair business practice, as set forth in California Business & Professions Code §§17200-17208.

161. Defendant has clearly established a policy of accepting a certain amount of collateral damage, as represented by the damages to Representative Plaintiffs and members of the California subclass herein alleged, as incidental to its business operations, rather than accept the alternative costs of full compliance with fair, lawful and honest business practices ordinarily borne by responsible competitors of Defendant and as set forth in legislation and the judicial record.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

162. Representative Plaintiffs and members of the California subclass request that this Court enter such orders or judgments as may be necessary to enjoin Defendant from continuing its unfair, unlawful, and/or deceptive practices and to restore to Representative Plaintiffs and members of the California subclass any money Defendant acquired by unfair competition, including restitution and/or restitutionary disgorgement, as provided in Cal. Bus. & Prof. Code §17200, et seq.; and for such other relief set forth below.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on behalf of themselves and each member of the proposed National Class and the California Subclass, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities in further violation of California Business and Professions Code §17200, *et seq.*;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiffs' and Class Members' PII/PHI, and from refusing to issue prompt, complete, any accurate disclosures to Representative Plaintiffs and Class Members;

5. For injunctive relief requested by Representative Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiffs and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. requiring Defendant to delete and purge the PII/PHI of Representative Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' PII/PHI;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Representative Plaintiffs' and Class Members' PII/PHI on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII/PHI, as well as protecting the PII/PHI of Representative Plaintiffs and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiffs, individually and on behalf of the Plaintiff Classes, hereby demand a trial by jury.

Dated: June 21, 2021

SCOTT COLE & ASSOCIATES, APC

By: */s/ Scott Edward Cole*
Scott Edward Cole, Esq.
Attorneys for Representative Plaintiffs

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

ClassAction.org