

1 Scott Edward Cole, Esq. (S.B. #160744)
2 Laura Grace Van Note, Esq. (S.B. #310160)
3 **SCOTT COLE & ASSOCIATES, APC**
4 555 12th Street, Suite 1725
5 Oakland, California 94607
6 Telephone: (510) 891-9800
7 Facsimile: (510) 891-7030
8 Email: scole@scalaw.com
9 Email: lvannote@scalaw.com
10 Web: www.scalaw.com

11 Attorneys for Representative Plaintiffs
12 and the Plaintiff Classes

13 **UNITED STATES DISTRICT COURT**
14 **SOUTHERN DISTRICT OF CALIFORNIA**

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

18 Plaintiffs,

19 vs.

20 SCRIPPS HEALTH,

21 Defendant.

22 Case No. '21CV1135 DMS RBB

23 **CLASS ACTION**

24 **COMPLAINT FOR DAMAGES,
25 RESTITUTION AND
26 INJUNCTIVE/EQUITABLE RELIEF**

27 **JURY TRIAL DEMANDED**

28 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

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

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

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

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

22
 23 ¹ Personally identifiable information generally incorporates information that can be used
 24 to distinguish or trace an individual’s identity, either alone or when combined with other
 25 personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all
 26 information that on its face expressly identifies an individual. PII also is generally defined to
 27 include certain identifiers that do not on their face name an individual, but that are considered
 28 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

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

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

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

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

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

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

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

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

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

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

24
25
26
27
28

JURISDICTION AND VENUE

1
2 13. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction)
3 and/or 28 U.S.C. §1331 (controversy arising under United States law). Specifically, this Court has
4 subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is
5 a class action where the amount in controversy exceeds the sum or value of \$5 million, exclusive
6 of interest and costs, there are more than 100 members in the proposed class, and at least one other
7 Class Member is a citizen of a state different from Defendant.

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

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

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

PLAINTIFFS

17
18
19 17. Representative Plaintiff Michael Rubenstein is an adult individual and resident of
20 the State of California. He is referred to in this Complaint simply as “Rubenstein” or, collectively
21 with his fellow plaintiff, as a “Representative Plaintiff.” Rubenstein is a victim of the Data Breach.

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

24 19. Rubenstein’s PII/PHI was exposed in the Data Breach because Scripps Health
25 stored and/or shared Rubenstein’s PII/PHI. In late April 2021, an unauthorized person gained
26 access to Defendant’s network, deployed malware, and, on April 29, 2021, acquired copies of
27 numerous documents/records within Defendant’s system. The PII/PHI included both personal and
28 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

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

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

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

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

22 23. Because of Rubenstein’s condition, he must constantly monitor his disease state
23 through the lab results accessible through Defendant’s patient portal and Epic EMR in order to
24 determine the proper administration of his ongoing prescribed medications. However, as a result
25 of the Data Breach, both the past lab results and future lab orders that Rubenstein had through July
26 2021 were inaccessible to him. Additionally, there were no alternative or backup systems in place
27 for Rubenstein to access his laboratory information since all of Defendant’s lab results and lab
28 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

27 37. Additionally, Representative Plaintiffs are very careful about sharing their PII/PHI,
28 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

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

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

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

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

17
18 **DEFENDANT**

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

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

26
27
28 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

1 43. Defendant's failure to protect Representative Plaintiffs and Class Members' data
 2 was not for lack of resources. In its fiscal year ending in September 2019, Defendant reported total
 3 revenue of \$3,345,481,577 and net revenue less expenses of \$274,752,677, with \$113,859,866 in
 4 investment income alone.⁵ In that same fiscal year, Defendant reported net assets of
 5 4,250,272,456.⁶

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

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

19 46. In addition to violating its purported commitment to its patients and community,
 20 Defendant's failure to adequately secure Representative Plaintiffs' and Class Members' sensitive
 21 data also breaches duties it owes Representative Plaintiffs and Class Members under statutory and
 22 common law. Under the Health Insurance Portability Act of 1996, healthcare providers have an
 23 affirmative duty to keep patients' Protected Health Information private. As a covered entity,
 24 Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard
 25

26 ⁵ 2018 990 Form available at
<https://projects.propublica.org/nonprofits/organizations/951684089>.

27 ⁶ *Id.*

28 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

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

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

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

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

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

24 ⁹ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B4-healthcare-08-00133> (citing
 25 Chernyshev, M., Zeadally, S. & Baig, Z. Healthcare Data Breaches: Implications for Digital
 Forensic Readiness. J Med Syst 43, 7 (2019).

26 ¹⁰ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4479128/>.

27 ¹¹ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133>.

28 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>.

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

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

9 51. The true names and capacities of persons or entities, whether individual, corporate,
 10 associate, or otherwise, who may be responsible for some of the claims alleged here are currently
 11 unknown to Representative Plaintiffs. Representative Plaintiffs will seek leave of court to amend
 12 this Complaint to reflect the true names and capacities of such other responsible parties when their
 13 identities become known.

CLASS ACTION ALLEGATIONS

14
 15
 16 52. Representative Plaintiffs bring this action pursuant to the provisions of Rules 23(a),
 17 (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the
 18 following classes/subclass(es) (collectively, the “Classes”):

19
 20 California class:

21 “All individuals within the State of California whose PII/PHI was stored by Defendant
 22 and/or was exposed to unauthorized third parties as a result of the compromise of Scripps
 23 Health’s data systems, as announced on or about June 1, 2021.”

24 National class:

25 “All individuals within the United States of America whose PII/PHI was stored by
 26 Defendant and/or was exposed to unauthorized third parties as a result of the compromise
 27 of Scripps Health’s data systems, as announced on or about June 1, 2021.”

28 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

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

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

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

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

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

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

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

1) Whether Defendant failed to implement adequate data security
measures allowed the Data Breach to occur;

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

3) 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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- 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

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

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

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

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

COMMON FACTUAL ALLEGATIONS

Defendant's Unlawful Conduct

13
 14
 15
 16 58. On May 1, 2021, Scripps Health identified unusual network activity and initiated
 17 its response protocols with the assistance of computer forensic firms. The investigation determined
 18 that an unauthorized person gained access to the network, deployed malware, and acquired copies
 19 of many of the documents on Defendant's system as early as April 29, 2021.

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

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

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

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

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

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

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

20 64. This complimentary service, however, does not and will not fully protect the
21 patients from cyber criminals and is largely ineffective against protecting data after it has been
22 stolen. Cyber criminals are fully aware of the well-publicized preventative measures taken by
23 entities after data breaches such as that which happened here and will, therefore, oftentimes hold
24 onto the stolen data and not use it until after the complimentary service is no longer active, and
25 long after victim concerns and preventative steps have diminished. Consistent with these realities,
26 Scripps Health' offer to provide a complimentary one-year membership of Experian
27 IdentityWorksSM Credit 3B will likely prove largely ineffectual in combating the misuse of
28 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

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

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

8 67. The announcement included the following:

9 On May 1, 2021, we identified unusual network activity. We immediately
10 initiated our incident response protocols, which included isolating
11 potentially impacted devices and shutting off select systems. We also began
12 an investigation with the assistance of computer forensic firms. The
13 investigation determined that an unauthorized person gained access to our
14 network, deployed malware, and, on April 29, 2021, acquired copies of
15 some of the documents on our system. On May 10, 2021, we discovered
16 that some of those documents contained patient information. Upon
17 conducting a review of those documents, we determined that one or more
18 files may have reflected your name, address, date of birth, health insurance
19 information, medical record number, patient account number, and/or
20 clinical information, such as physician name, date(s) of service, and/or
21 treatment information.

22 We have no indication that any of your information has been used to commit
23 fraud. However, we recommend that you review the statements you receive
24 from your healthcare providers and health insurer. If you see any medical
25 services that you did not receive, please call the provider or insurer
26 immediately. To help prevent something like this from happening again, we
27 are continuing to implement enhancements to our information security,
28 systems, and monitoring capabilities.¹⁷

20 68. Despite this notification, Representative Plaintiffs and the Class Members remain,
21 even today, in the dark regarding what data was stolen, the particular malware used, and what steps
22 are being taken to secure their PII/PHI going forward. Indeed, even the particular “computer
23 forensic firms” being employed is left a mystery, such that the quality of that forensic work is left
24 in question. Especially in light of Defendant’s suggestion that patients “review the statements
25 [they] receive from [their] healthcare providers and health insurer[s],” Representative Plaintiffs
26 and Class Members are left to speculate as to the full impact of the Data Breach and how exactly
27
28

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

1 Defendant intends to “enhance” its information security, systems, and monitoring capabilities so
2 as to prevent further breaches.

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

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

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

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

17
18 **Defendant Maintained Representative Plaintiffs’ and Class Members’ PII/PHI**

19 73. Defendant acquired, collected, and stored Representative Plaintiffs’ and Class
20 Members’ PII/PHI.

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

25 75. Indeed, personal health records can improve patient engagement, coordinate and
26 combine information from multiple healthcare providers, ensure availability of patient information
27 online, reduce administrative costs and enhance provider-patient communication.
28

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

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

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

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

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

15 80. The healthcare industry has experienced a large number of high-profile cyber-
 16 attacks even in just the one-year period preceding the filing of this Complaint and cyber-attacks,
 17 generally, have become increasingly more common. More healthcare data breaches were reported
 18 in 2020 than in any other year, showing a 25% increase.¹⁸ Additionally, according to the HIPAA
 19 Journal, the largest healthcare data breaches have been reported in April 2021.¹⁹

20 81. For example, one of Scripps Health's competitors, Universal Health Services,
 21 experienced a cyber-attack on September 29, 2020 that was very similar to the attack on Scripps
 22 Health. Not unlike Scripps Health, Universal Health Services suffered a four-week outage of its
 23 systems which caused as much as \$67 million in recovery costs and lost revenue.²⁰ Due to the
 24 high-profile nature of the Universal Health Services breach, and other breaches of its kind, Scripps
 25

26 ¹⁸ <https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/> (last accessed June 17,
 2021).

27 ¹⁹ <https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/> (last accessed June
 17, 2021).

28 ²⁰ [https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-
 reports-2020-fourth-quarter-and](https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and) (last accessed June 17, 2021).

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

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

7
 8 **Value of Personal Identifiable Information**

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

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

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

22 86. The Federal Trade Commission ("FTC") defines identity theft as "a fraud
 23 committed or attempted using the identifying information of another person without authority."²¹
 24 The FTC describes "identifying information" as "any name or number that may be used, alone or
 25 in conjunction with any other information, to identify a specific person," including, among other
 26 things, "[n]ame, Social Security number, date of birth, official State or government issued driver's
 27

28
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

1 license or identification number, alien registration number, government passport number,
 2 employer or taxpayer identification number.”²²

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

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

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

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

26 91. As such, the PII/PHI of individuals remains of high value to criminals, as evidenced
 27 by the prices they will pay through the dark web. Numerous sources cite dark web pricing for
 28

²² *Id.*

1 | stolen identity credentials. For example, personal information can be sold at a price ranging from
2 | \$40 to \$200, and bank details have a price range of \$50 to \$200.²³ Experian reports that a stolen
3 | credit or debit card number can sell for \$5 to \$110 on the dark web.²⁴ Criminals can also purchase
4 | access to entire company data breaches from \$999 to \$4,995.²⁵

5 | 92. Social Security numbers, for example, are among the worst kind of personal
6 | information to have stolen because they may be put to a variety of fraudulent uses and are difficult
7 | for an individual to change. The Social Security Administration stresses that the loss of an
8 | individual's Social Security number, as is the case here, can lead to identity theft and extensive
9 | financial fraud:

10 | A dishonest person who has your Social Security number can use it to get
11 | other personal information about you. Identity thieves can use your number
12 | and your good credit to apply for more credit in your name. Then, they use
13 | the credit cards and don't pay the bills, it damages your credit. You may not
14 | find out that someone is using your number until you're turned down for
15 | credit, or you begin to get calls from unknown creditors demanding
16 | payment for items you never bought. Someone illegally using your Social
17 | Security number and assuming your identity can cause a lot of problems.²⁶

18 | 93. What is more, it is no easy task to change or cancel a stolen Social Security number.
19 | An individual cannot obtain a new Social Security number without significant paperwork and
20 | evidence of actual misuse. In other words, preventive action to defend against the possibility of
21 | misuse of a Social Security number is not permitted; an individual must show evidence of actual,
22 | ongoing fraud activity to obtain a new number.

23 | 94. Even then, a new Social Security number may not be effective. According to Julie
24 | Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the
25 |

26 | ²³ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct.
27 | 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).

28 | ²⁴ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.
29 | 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

1 new number very quickly to the old number, so all of that old bad information is quickly inherited
2 into the new Social Security number.”²⁷

3 95. Based on the foregoing, the information compromised in the Data Breach is
4 significantly more valuable than the loss of, for example, credit card information in a retailer data
5 breach, because, there, victims can cancel or close credit and debit card accounts.

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

9 97. This data demands a much higher price on the black market. Martin Walter, senior
10 director at cybersecurity firm RedSeal, explained, “Compared to credit card information,
11 personally identifiable information and Social Security numbers are worth more than 10x on the
12 black market.”²⁸

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

15 99. The PII/PHI of Representative Plaintiffs and Class Members was taken by hackers
16 to engage in identity theft or to sell it to other criminals who will purchase the PII/PHI for that
17 purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

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

21 [L]aw enforcement officials told us that in some cases, stolen data may be
22 held for up to a year or more before being used to commit identity theft.
23 Further, once stolen data have been sold or posted on the Web, fraudulent
24 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

25 ²⁷ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR
26 (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).

27 ²⁸ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card
28 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

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

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

- 11 a. unauthorized use of their Personal Information;
- 12 b. theft of their personal and financial information;
- 13 c. costs associated with the detection and prevention of identity theft and
14 unauthorized use of their financial accounts;
- 15 d. damages arising from the inability to use their Personal Information;
- 16 e. loss of privacy, and embarrassment;
- 17 f. costs associated with time spent and the loss of productivity or the
18 enjoyment of one’s life from taking time to address and attempt to
19 ameliorate, mitigate and deal with the actual and future consequences of the
20 Data Breach, including finding fraudulent charges, purchasing credit
21 monitoring and identity theft protection services, and the stress, nuisance
22 and annoyance of dealing with all issues resulting from the Data Breach;
- 23 g. the imminent and certainly impending injury flowing from potential fraud
24 and identify theft posed by their Personal Information being placed in the
25 hands of criminals and already misused via the sale of Representative
26 Plaintiffs’ and Class Members’ information on the Internet black market;
- 27 h. damages to and diminution in value of their Personal Information entrusted
28 to Defendant for the sole purpose of purchasing products and services from
Defendant; and the loss of Representative Plaintiffs’ and Class Members’
privacy.

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

28 _____
<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

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

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

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

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

17
18 **FIRST CLAIM FOR RELIEF**
19 **NEGLIGENCE**
 (Both Classes)

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

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

28

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

1 110. Among these duties, Defendant was expected:
2 a. to exercise reasonable care in obtaining, retaining, securing, safeguarding,
3 deleting and protecting Personal Information in its possession;
4 b. to protect Personal Information using reasonable and adequate security
5 procedures and systems that are compliant with industry-standard practices;
6 and
7 c. to implement processes to quickly detect the Data Breach and to timely act
8 on warnings about data breaches.
9 111. Defendant knew that the Personal Information was private and confidential and
10 should be protected as private and confidential and, thus, Defendant owed a duty of care not to
11 subject Representative Plaintiffs and Class Members to an unreasonable risk of harm because they
12 were foreseeable and probable victims of any inadequate security practices.
13 112. Defendant knew, or should have known, of the risks inherent in collecting and
14 storing Personal Information, the vulnerabilities of its data security systems, and the importance
15 of adequate security. Defendant knew about numerous, well-publicized data breaches.
16 113. Defendant knew, or should have known, that its data systems and networks did not
17 adequately safeguard Representative Plaintiffs' and/or Class Members' Personal Information.
18 114. Defendant breached its duties to Representative Plaintiffs and Class Members by
19 failing to provide fair, reasonable, or adequate computer systems and data security practices to
20 safeguard Personal Information of Representative Plaintiffs and Class Members.
21 115. Because Defendant knew that a breach of its systems would damage hundreds of
22 thousands of individuals, including Representative Plaintiffs and Class Members, Defendant had
23 a duty to adequately protect its data systems and the Personal Information contained thereon.
24 116. Representative Plaintiffs' and Class Members' willingness to entrust Defendant
25 with their Personal Information was predicated on the understanding that Defendant would take
26 adequate security precautions. Moreover, only Defendant had the ability to protect its systems and
27 the Personal Information its stored on them from attack.
28 117. 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

1 118. Defendant also had independent duties under state and federal laws that required
2 Defendant to reasonably safeguard Representative Plaintiffs’ and Class Members’ Personal
3 Information and promptly notify them about the Data Breach. These “independent duties” are
4 untethered to any contract between Defendant and Representative Plaintiffs and/or Class
5 Members.

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

- 8 a. by failing to provide fair, reasonable, or adequate computer systems and
9 data security practices to safeguard Personal Information of Representative
10 Plaintiffs and Class Members;
- 11 b. by failing to timely and accurately disclose that Representative Plaintiffs’
12 and Class Members’ Personal Information had been improperly acquired or
13 accessed;
- 14 c. by failing to adequately protect and safeguard Personal Information by
15 knowingly disregarding standard information security principles, despite
16 obvious risks, and by allowing unmonitored and unrestricted access to
17 unsecured Personal Information;
- 18 d. by failing to provide adequate supervision and oversight of the Personal
19 Information with which it was and is entrusted, in spite of the known risk
20 and foreseeable likelihood of breach and misuse, which permitted an
21 unknown third party to gather Personal Information of Representative
22 Plaintiffs and Class Members, misuse the Personal Information and
23 intentionally disclose it to others without consent.

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

28 121. 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

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

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

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

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

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

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

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

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

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

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

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

21
22 **SECOND CLAIM FOR RELIEF**
23 **INVASION OF PRIVACY**
(Both Classes)

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

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

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

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

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

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

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

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

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

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

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

27
28

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

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

3 147. The breach of the personal data of well over one hundred thousand Defendant
4 patients instituted a “breach of the security system” of Defendant pursuant to Civil Code
5 §1798.82(g).

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

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

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

16 151. Accordingly, Representative Plaintiffs requests that the Court enter an injunction
17 requiring Defendant to implement and maintain reasonable security procedures to protect patients’
18 data in compliance with the California Customer Records Act, including, but not limited to: (1)
19 ordering that Defendant, consistent with industry standard practices, engage third party security
20 auditors/penetration testers as well as internal security personnel to conduct testing, including
21 simulated attacks, penetration tests, and audits on Defendant’s systems on a periodic basis; (2)
22 ordering that Defendant engage third party security auditors and internal personnel, consistent with
23 industry standard practices, to run automated security monitoring; (3) ordering that Defendant
24 audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering
25 that Defendant, consistent with industry standard practices, conduct regular database scanning and
26 securing checks; (5) ordering that Defendant, consistent with industry standard practices,
27 periodically conduct internal training and education to inform internal security personnel how to
28

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

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

3 152. Representative Plaintiffs further request that the Court require Defendant to (1)
4 identify and notify all members of the California subclass who have not yet been informed of the
5 Data Breach; and (2) to notify affected former and current patients of any future data breaches by
6 email within 24 hours of Defendant’s discovery of a breach or possible breach and by mail within
7 72 hours.

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

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

17
18 **FOURTH CLAIM FOR RELIEF**
19 **UNFAIR BUSINESS PRACTICES (CAL. BUS. & PROF. CODE, §17200, ET SEQ.)**
20 **(California Subclass Only)**

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

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

26 157. The knowing conduct of Defendant, as alleged herein, constitutes an unlawful
27 and/or fraudulent business practice, as set forth in California Business & Professions Code
28 §§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

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

- 3 a. failure to maintain adequate computer systems and data security practices
4 to safeguard Personal Information;
- 5 b. failure to disclose that its computer systems and data security practices were
6 inadequate to safeguard Personal Information from theft;
- 7 c. failure to timely and accurately disclose the Data Breach to Representative
8 Plaintiffs and members of the California subclass;
- 9 d. continued acceptance of Personal Information and storage of other personal
10 information after Defendant knew or should have known of the security
11 vulnerabilities of the systems that were exploited in the Data Breach; and
- 12 e. continued acceptance of Personal Information and storage of other personal
13 information after Defendant knew or should have known of the Data Breach
14 and before it allegedly remediated the Breach.

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

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

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

26 161. Defendant has clearly established a policy of accepting a certain amount of
27 collateral damage, as represented by the damages to Representative Plaintiffs and members of the
28 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.

1 162. Representative Plaintiffs and members of the California subclass request that this
2 Court enter such orders or judgments as may be necessary to enjoin Defendant from continuing its
3 unfair, unlawful, and/or deceptive practices and to restore to Representative Plaintiffs and
4 members of the California subclass any money Defendant acquired by unfair competition,
5 including restitution and/or restitutionary disgorgement, as provided in Cal. Bus. & Prof. Code
6 §17200, et seq.; and for such other relief set forth below.

7
8 **RELIEF SOUGHT**

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

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

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

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

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

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

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

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

- 1 b. requiring Defendant to protect, including through encryption, all data
- 2 collected through the course of business in accordance with all applicable
- 3 regulations, industry standards, and federal, state or local laws;
- 4 c. requiring Defendant to delete and purge the PII/PHI of Representative
- 5 Plaintiffs and Class Members unless Defendant can provide to the Court
- 6 reasonable justification for the retention and use of such information when
- 7 weighed against the privacy interests of Representative Plaintiffs and Class
- 8 Members;
- 9 d. requiring Defendant to implement and maintain a comprehensive
- 10 Information Security Program designed to protect the confidentiality and
- 11 integrity of Representative Plaintiffs’ and Class Members’ PII/PHI;
- 12 e. requiring Defendant to engage independent third-party security auditors and
- 13 internal personnel to run automated security monitoring, simulated attacks,
- 14 penetration tests, and audits on Defendant’s systems on a periodic basis;
- 15 f. prohibiting Defendant from maintaining Representative Plaintiffs’ and
- 16 Class Members’ PII/PHI on a cloud-based database;
- 17 g. requiring Defendant to segment data by creating firewalls and access
- 18 controls so that, if one area of Defendant’s network is compromised,
- 19 hackers cannot gain access to other portions of Defendant’s systems;
- 20 h. requiring Defendant to conduct regular database scanning and securing
- 21 checks;
- 22 i. requiring Defendant to establish an information security training program
- 23 that includes at least annual information security training for all employees,
- 24 with additional training to be provided as appropriate based upon the
- 25 employees’ respective responsibilities with handling PII/PHI, as well as
- 26 protecting the PII/PHI of Representative Plaintiffs and Class Members;
- 27 j. requiring Defendant to implement a system of tests to assess its respective
- 28 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;

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

3 **JURY DEMAND**

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

6
7 Dated: June 21, 2021

SCOTT COLE & ASSOCIATES, APC

8
9 By: /s/ Scott Edward Cole
10 Scott Edward Cole, Esq.
11 Attorneys for Representative Plaintiffs

12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12th STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800