

1 Scott Edward Cole, Esq. (S.B. #160744)
2 Laura Grace Van Note, Esq. (S.B. #310160)
3 Julia Deutsch, Esq. (S.B. #278163)
4 **COLE & VAN NOTE**
5 555 12th Street, Suite 1725
6 Oakland, California 94607
7 Telephone: (510) 891-9800
8 Facsimile: (510) 891-7030
9 Email: sec@colevannote.com
10 Email: lvn@colevannote.com
11 Email: jkd@colevannote.com
12 Web: www.colevannote.com

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego
08/26/2022 at 10:38:27 AM
Clerk of the Superior Court
By Brandon Krause, Deputy Clerk

13 Attorneys for Representative Plaintiff Florencio Ramos
14 and the Plaintiff Class

15 **IN THE SUPERIOR COURT OF THE STATE OF CALIFORNIA**
16 **IN AND FOR THE COUNTY OF SAN DIEGO**

17 FLORENCIO RAMOS, individually, and
18 on behalf of all others similarly situated,

19 Plaintiff,

20 vs.

21 SAN DIEGO AMERICAN INDIAN
22 HEALTH CENTER, and DOES 1 through
23 100, inclusive,

24 Defendants.

Case No. 37-2022-00034482-CU-NP-CTL

CLASS ACTION

**COMPLAINT FOR DAMAGES,
INJUNCTIVE AND EQUITABLE RELIEF
FOR:**

1. NEGLIGENCE;
2. CONFIDENTIALITY OF MEDICAL INFORMATION ACT (CAL. CIV. CODE §56);
3. INVASION OF PRIVACY;
4. BREACH OF CONFIDENCE;
5. BREACH OF IMPLIED CONTRACT;
6. BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING;
7. UNFAIR BUSINESS PRACTICES;
8. UNJUST ENRICHMENT

[JURY TRIAL DEMANDED]

25
26
27 Representative Plaintiff alleges as follows:
28

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

INTRODUCTION

1
2 1. Representative Plaintiff Florencio Ramos (“Ramos” or “Representative Plaintiff”)
3 brings this class action against Defendant San Diego American Indian Health Center (“Defendant”
4 or “SDAIHC”) for its failure to properly secure and safeguard Representative Plaintiff’s and Class
5 Members’ personally identifiable information stored within Defendant’s information network,
6 including, without limitation, their full names, addresses, dates of birth, claims information (e.g.,
7 date and cost of health care services and claims identifiers), laboratory results, medical diagnoses
8 and conditions, Medical Record Numbers and other medical identifiers, prescription information,
9 treatment information, medical information (these types of information, *inter alia*, being hereafter
10 referred to, collectively, as “personal health information” or “PHI”),¹ email addresses, fax
11 numbers, Social Security numbers, government identification numbers, payment card numbers or
12 financial account numbers and security codes, and usernames and passwords (these latter types of
13 information, *inter alia*, being hereafter referred to, collectively, as “personally identifiable
14 information” or “PII”),² and to properly secure and safeguard Representative Plaintiff’s and Class
15 Members’ PHI and PII stored within Defendant’s information network.

16 2. With this action, Representative Plaintiff seeks to hold Defendant responsible for
17 the harms it caused and will continue to cause Representative Plaintiff and the countless other
18 similarly situated persons in the massive and preventable cyberattack that occurred on or about
19 May 5, 2022, by which cybercriminals infiltrated Defendant’s inadequately protected network
20 servers and accessed highly sensitive PHI/PII and financial information which was being kept
21 unprotected (the “Data Breach”).

22
23 ¹ Personal health information (“PHI”) is a category of information that refers to an individual’s
24 medical records and history, which is protected under the Health Insurance Portability and
25 Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses,
26 personal or family medical histories and data points applied to a set of demographic information
27 for a particular patient.

28 ² Personally identifiable information (“PII”) 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).

1 3. Representative Plaintiff further seeks to hold Defendant responsible for not
2 ensuring that the PHI/PII was maintained in a manner consistent with industry, the Health
3 Insurance Portability and Accountability Act of 1996 (“HIPPA”) Privacy Rule (45 CFR, Parts 160
4 and 164(A) and (E)), the HIPPA Security Rule (45 CFR, Parts 160 and 164(A) and (C)), and other
5 relevant standards.

6 4. While Defendant claims to have known about the Data Breach as early as May 5,
7 2022, it did not immediately report the security incident to Representative Plaintiff or Class
8 Members. Indeed, Representative Plaintiff and Class Members were wholly unaware of the Data
9 Breach until he/they received letter(s) from Defendant informing them of it. In particular, the letter
10 Representative Plaintiff received was dated August 15, 2022.

11 5. Defendant acquired, collected and stored Representative Plaintiff’s and Class
12 Members’ PHI/PII and/or financial information to provide efficient and quality healthcare,
13 employment and/or pharmacy services to Representative Plaintiff and/or Class Members.
14 Therefore, at all relevant times, Defendant knew, or should have known, that Representative
15 Plaintiff and Class Members would use Defendant’s networks to store and/or share sensitive data,
16 including highly confidential PHI/PII, because Defendant promised them that creating personal
17 healthcare and/or employment records would improve care quality and/or employment services.

18 6. HIPAA establishes national minimum standards for the protection of individuals’
19 medical records and other personal health information. HIPAA, generally, applies to health plans,
20 health care clearinghouses, and those health care providers that conduct certain health care
21 transactions electronically, and sets minimum standards for Defendant’s maintenance of
22 Representative Plaintiff’s and Class Members’ PHI/PII. More specifically, HIPAA requires
23 appropriate safeguards be maintained by healthcare providers such as Defendant to protect the
24 privacy of personal health information and sets limits and conditions on the uses and disclosures
25 that may be made of such information without customer/patient authorization. HIPAA also
26 establishes a series of rights over Representative Plaintiff’s and Class Members’ PHI/PII, including
27 rights to examine and obtain copies of their health records, and to request corrections thereto.
28

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

6 8. By obtaining, collecting, using, and deriving a benefit from Representative
7 Plaintiff’s and Class Members’ PHI/PII, Defendant assumed legal and equitable duties to those
8 individuals. These duties arise from HIPAA and other state and federal statutes and regulations as
9 well as common law principles. Representative Plaintiff does not bring claims in this action for
10 direct violations of HIPAA, but charges Defendant with various legal violations merely predicated
11 upon the duties set forth in HIPAA.

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

23
24
25 **JURISDICTION AND VENUE**

26 10. This Court has jurisdiction over Representative Plaintiff’s and Class Members’
27 claims for damages and injunctive relief pursuant to, *inter alia*, Cal. Civ. Code §56, *et seq.*, §1798,
28 *et seq.* and Cal. Bus. & Prof. Code §17200, *et seq.*, among other California state statutes.

1 11. Venue as to Defendant is proper in this judicial district pursuant to California Code
2 of Civil Procedure § 395(a). Defendant provided the aforementioned services within this County
3 to numerous Class Members and transacts business, has agents, and is otherwise within this
4 Court’s jurisdiction for purposes of service of process. The unlawful acts alleged herein have had
5 a direct effect on Representative Plaintiff and those similarly situated within the State of California
6 and within this County.

7
8 **PLAINTIFF(S)**

9 12. Representative Plaintiff is an adult individual and, at all relevant times herein, a
10 resident of the State of California. Representative Plaintiff is a victim of the Data Breach.

11 13. Prior to the Data Breach, Defendant was Representative Plaintiff’s primary care
12 provider. In order to receive medical services from Defendant, Representative Plaintiff provided
13 Defendant with highly sensitive personal, medical, and financial information. As a result,
14 Representative Plaintiff’s information was among the data accessed by an unauthorized third party
15 in the Data Breach.

16 14. Representative Plaintiff received—and was a “consumer” for purposes of
17 obtaining—medical services from Defendant within the State of California.

18 15. At all times herein relevant, Representative Plaintiff is and was a member of the
19 Class.

20 16. As required in order to obtain medical services from Defendant, Representative
21 Plaintiff provided Defendant with highly sensitive personal, financial, health and insurance
22 information.

23 17. Representative Plaintiff’s PHI/PII was exposed in the Data Breach because
24 Defendant stored and/or shared Representative Plaintiff’s PHI/PII and financial information. His
25 PHI/PII and financial information was within the possession and control of Defendant at the time
26 of the Data Breach.

27 18. Representative Plaintiff received a letter from Defendant, dated August 15, 2022,
28 informing him that his PHI/PII and/or financial information was involved in the Data Breach (the

1 “Notice”). The Notice explained that Defendant shut down many of its systems after detecting
2 unusual activity, but not until an unauthorized third party gained access to Defendant’s network
3 and accessed Representative Plaintiff’s PHI/PII and financial information. While Defendant
4 claims to have known of this breach on May 5, 2022, it did not inform Representative Plaintiff of
5 this breach until August 15, 2022.

6 19. As a result, Representative Plaintiff spent time dealing with the consequences of
7 the Data Breach, which included and continues to include, time spent verifying the legitimacy and
8 impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-
9 monitoring his accounts and seeking legal counsel regarding his options for remedying and/or
10 mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

11 20. Representative Plaintiff suffered actual injury in the form of damages to and
12 diminution in the value of his PHI/PII—a form of intangible property that he entrusted to
13 Defendant for the purpose of obtaining health services, which was compromised in and as a result
14 of the Data Breach.

15 21. Representative Plaintiff suffered lost time, annoyance, interference, and
16 inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss
17 of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PHI/PII
18 and/or financial information.

19 22. Representative Plaintiff has suffered imminent and impending injury arising from
20 the substantially increased risk of fraud, identity theft, and misuse resulting from his PHI/PII and
21 financial information, in combination with his name, being placed in the hands of unauthorized
22 third-parties/criminals.

23 23. Representative Plaintiff has a continuing interest in ensuring that his PHI/PII and
24 financial information, which, upon information and belief, remains backed up in Defendant’s
25 possession, is protected and safeguarded from future breaches.

26
27
28

DEFENDANT

24. Defendant is a California nonprofit corporation with a principal place of business located at 2630 First Avenue, San Diego, CA 92103

25. Defendant was founded in 1979 to provide healthcare to members of the San Diego and larger community, with emphasis on the American Indian community and taking a culturally-informed approach. Defendant provides comprehensive medical, dental, behavioral health, and community wellness services, while respecting customs and traditions of American Indians.³

26. Defendant's failure to safeguard its patients' data is particularly troubling considering that Defendant's patients are primarily the marginalized American Indian community members and individuals who may lack the resources and leisure time to fully explore and take remedial action. Many cannot afford expensive credit monitoring and will not be able to take time off work to address their stolen identities and/or other fraud which may be committed in their name. Accordingly, the Data Breach is likely to have particularly severe real-world consequences, relative to other similar events. Defendant's patients are already among the most vulnerable members of our society, and Defendant's failure to protect their sensitive data has made them even more so.

27. 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 Plaintiff. Representative Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

28. Representative Plaintiff brings this action individually and on behalf of all persons similarly situated and proximately damaged by Defendant's conduct including, but not necessarily limited to, the following Plaintiff Class:

³ <https://sdaihc.org/about-us/#mv> (last accessed August 25, 2022).

1 “All individuals within the State of California whose PHI/PII and/or
2 financial information was stored by Defendant and was exposed to
3 unauthorized third-parties as a result of the data breach discovered
4 by Defendant on or around May 5, 2022.”

5 29. Excluded from the Class are the following individuals and/or entities: (a) Defendant
6 and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which
7 Defendant has a controlling interest; (b) all individuals who make a timely election to be excluded
8 from this proceeding using the correct protocol for opting out; (c) any and all federal, state or local
9 governments, including but not limited to its departments, agencies, divisions, bureaus, boards,
10 sections, groups, counsels and/or subdivisions; and (d) all judges assigned to hear any aspect of
11 this litigation, as well as their immediate family members.

12 30. Representative Plaintiff reserves his right to request additional subclasses be added,
13 as necessary, based on the types of PHI/PII and financial information that were compromised
14 and/or the nature of certain Class Members’ relationship(s) to the Defendant. At present, Class
15 Members include, *inter alia*, current and former California employees and patients of Defendant.

16 31. Representative Plaintiff reserves the right to amend the above definition in
17 subsequent pleadings and/or motions for class certification.

18 32. This action has been brought and may properly be maintained as a class action
19 under California Code of Civil Procedure § 382 because there is a well-defined community of
20 interest in the litigation and the proposed class is easily ascertainable.

21 a. Numerosity: A class action is the only available method for the fair and
22 efficient adjudication of this controversy. The members of the Plaintiff
23 Class are so numerous that joinder of all members is impractical, if not
24 impossible. Representative Plaintiff is informed and believes and, on that
25 basis, alleges that the total number of Class Members is in the hundreds of
26 thousands of individuals. Membership in the Class will be determined by
27 analysis of Defendant’s records.

28 b. Commonality: Representative Plaintiff and 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 engaged in the wrongful conduct alleged
herein;

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

- 2) Whether Defendant had a legal duty to Representative Plaintiff and Class Members to exercise due care in collecting, storing, using and/or safeguarding their PHI/PII and financial information;
- 3) Whether Defendant knew or should have known of the susceptibility of Defendant's data security systems to a data breach;
- 4) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;
- 5) Whether Defendant's failure to implement adequate data security measures, including the sharing of Representative Plaintiff's and Class Members' PHI/PII and financial information allowed the Data Breach to occur and/or worsened its effects;
- 6) Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- 7) Whether Defendant adequately, promptly, and accurately informed Representative Plaintiff and Class Members that their PHI/PII and financial information had been compromised;
- 8) How and when Defendant actually learned of the Data Breach;
- 9) Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Representative Plaintiff and Class Members;
- 10) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of these systems, resulting in the loss of the PHI/PII and financial information of Representative Plaintiff and Class Members;
- 11) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- 12) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach and/or damages flowing therefrom;
- 13) Whether Defendant's actions alleged herein constitute gross negligence and whether the negligence/recklessness of any one or more individual(s) can be imputed to Defendant;
- 14) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI/PII and financial information of Representative Plaintiff and Class Members;

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

15) Whether Representative Plaintiff 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 and, if so, what is necessary to redress the imminent and currently ongoing harm faced by Representative Plaintiff, Class Members and the general public;

16) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

17) Whether Defendant continue to breach duties to Representative Plaintiff and Class Members.

c. Typicality: The Representative Plaintiff's claims are typical of the claims of the Plaintiff Class. Representative Plaintiff and all members of the Plaintiff Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein. The same event and conduct that gave rise to Representative Plaintiff's claims are identical to those that give rise to the claims of every Class Member because Representative Plaintiff and each Class Member had his/her sensitive PHI/PII and/or financial information compromised in the same way by the same conduct of Defendant. Representative Plaintiff and all Class Members face the identical threats resulting from the breach of his/her PHI/PII and/or financial information without the protection of encryption and adequate monitoring of user behavior and activity necessary to identify those threats.

d. Adequacy of Representation: Representative Plaintiff is an adequate representative of the Plaintiff Class in that Representative Plaintiff has the same interest in the litigation of this case as the remaining Class Members, is committed to vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the class in its entirety. Representative Plaintiff anticipates no management difficulties in this litigation. Representative Plaintiff and his counsel will fairly and adequately protect the interests of all Class Members.

e. Superiority of Class Action: The damages suffered by individual Class Members, are significant, but may be small relative to the enormous expense of individual litigation by each member. This makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought, by each individual member of the Plaintiff Class, 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

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

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. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

33. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, 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 Class in its entirety. Defendant’s policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiff’s challenge of these policies and practices hinges on Defendant’s conduct with respect to the Class in its entirety, not on facts or law applicable only to the Representative Plaintiff.

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

COMMON FACTUAL ALLEGATIONS

The Cyberattack

35. According to Defendant’s notice: On May 5, 2022, Defendant detected unusual activity on its network, forcing it to take all of its systems offline. An investigation found evidence of an unauthorized third party having accessed Defendant’s network, which stored Class Members’ PHI/PII and financial information.

36. In the course of the Data Breach, one or more unauthorized third-parties accessed Class Members’ sensitive data including, but not limited to: names, mailing addresses, Social Security numbers, dates of birth, demographic information, and medical information. Representative Plaintiff was among the individuals whose data was accessed in the Data Breach.

1 37. According to the Data Breach Notification which Defendant filed with Office of
2 the Maine Attorney General, 656,047 persons were affected by the Data Breach.⁴

3 38. Representative Plaintiff was provided the information detailed above upon his
4 receipt of a letter from Defendant, dated August 15, 2022. He was not aware of the Data Breach
5 until receiving that letter.

6
7 **Defendant's Failed Response to the Breach**

8 39. Not until roughly two weeks after it claims to have discovered the Data Breach did
9 Defendant begin sending the Notice to persons whose PHI/PII and/or financial information
10 Defendant confirmed was potentially compromised as a result of the Data Breach. The Notice
11 provided basic details of the Data Breach and Defendant's recommended next steps, such as
12 reviewing statements received from healthcare providers and insurers.

13 40. The Notice included, *inter alia*, the claims that Defendant had learned of the Data
14 Breach on May 5, 2022, had taken steps to respond, and was continuing to investigate. It also
15 stated that, "[u]pon detecting this incident we moved quickly to initiate a response, which included
16 conducting an investigation with the assistance of cybersecurity experts, confirming the security
17 of our network environment, and notifying law enforcement." It further provided that Defendant
18 has "reviewed and altered its policies and procedures relating to the security of our systems and
19 servers, and reviewed and altered how we manage data within our network."

20 41. Defendant sent a sample notice of data breach letter that mirrored the language of
21 the Notice sent to Representative Plaintiff and Class Members to the California Attorney General's
22 Office on October 26, 2021.⁵

23 42. Upon information and belief, the unauthorized third-party cybercriminals gained
24 access to Representative Plaintiff's and Class Members' PHI/PII and financial information with
25

26 ⁴ <https://apps.web.maine.gov/online/aeviewer/ME/40/219cad16-9e33-47b6-9cdf-0e9949e25aa6.shtml> (last accessed November 5, 2021).

27 ⁵ https://oag.ca.gov/privacy/databreach/list?field_sb24_org_name_value=community+medical+centers&field_sb24_breach_date_value%5Bmin%5D%5Bdate%5D=&field_sb24_breach_date_value%5Bmax%5D%5Bdate%5D= (last accessed November 3, 2021).

1 the intent of engaging in misuse of the PHI/PII and financial information, including marketing and
2 selling Representative Plaintiff's and Class Members' PHI/PII and financial information.

3 43. Defendant had and continues to have obligations created by HIPAA, the California
4 Confidentiality of Medical Information Act ("CMIA"), reasonable industry standards, common
5 law, state statutory law, and its own assurances and representations to keep Representative
6 Plaintiff's and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized
7 access.

8 44. Representative Plaintiff and Class Members were required to provide their PHI/PII
9 and financial information to Defendant with the reasonable expectation and mutual understanding
10 that Defendant would comply with its obligations to keep such information confidential and secure
11 from unauthorized access.

12 45. Despite this, Representative Plaintiff and the Class Members remain, even today,
13 in the dark regarding what particular data was stolen, the particular malware used, and what steps
14 are being taken, if any, to secure their PHI/PII and financial information going forward.
15 Representative Plaintiff and Class Members are left to speculate as to the full impact of the Data
16 Breach and how exactly Defendant intends to enhance its information security systems and
17 monitoring capabilities so as to prevent further breaches.

18 46. Representative Plaintiff's and Class Members' PHI/PII and financial information
19 may end up for sale on the dark web, or simply fall into the hands of companies that will use the
20 detailed PHI/PII and financial information for targeted marketing without the approval of
21 Representative Plaintiff and/or Class Members. Either way, unauthorized individuals can now
22 easily access the PHI/PII and/or financial information of Representative Plaintiff and Class
23 Members.

24
25 **Defendant Collected/Stored Class Members' PHI/PII and Financial Information**

26 47. Defendant acquired, collected, and stored and assured reasonable security over
27 Representative Plaintiff's and Class Members' PHI/PII and financial information.

28

1 48. As a condition of its relationships with Representative Plaintiff and Class Members,
2 Defendant required that Representative Plaintiff and Class Members entrust Defendant with highly
3 sensitive and confidential PHI/PII and financial information.

4 49. By obtaining, collecting, and storing Representative Plaintiff's and Class Members'
5 PHI/PII and financial information, Defendant assumed legal and equitable duties and knew or
6 should have known that they were thereafter responsible for protecting Representative Plaintiff's
7 and Class Members' PHI/PII and financial information from unauthorized disclosure.

8 50. Representative Plaintiff and Class Members have taken reasonable steps to
9 maintain the confidentiality of their PHI/PII and financial information. Representative Plaintiff
10 and Class Members relied on Defendant to keep their PHI/PII and financial information
11 confidential and securely maintained, to use this information for business and healthcare purposes
12 only, and to make only authorized disclosures of this information.

13 51. Defendant could have prevented the Data Breach by properly securing and
14 encrypting and/or more securely encrypting its servers generally, as well as Representative
15 Plaintiff's and Class Members' PHI/PII and financial information.

16 52. Defendant's negligence in safeguarding Representative Plaintiff's and Class
17 Members' PHI/PII and financial information is exacerbated by repeated warnings and alerts
18 directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks
19 in recent years.

20 53. The healthcare industry has experienced a large number of high-profile
21 cyberattacks even in just the one-year period preceding the filing of this Complaint and
22 cyberattacks, generally, have become increasingly more common. More healthcare data breaches
23 were reported in 2020 than in any other year, showing a 25% increase.⁶ Additionally, according to
24 the HIPAA Journal, the largest healthcare data breaches have been reported in April 2021.⁷

25
26
27 ⁶ <https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/> (last accessed
November 5, 2021).

28 ⁷ <https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/> (last accessed
November 5, 2021).

1 54. For example, Universal Health Services experienced a cyberattack on September
2 29, 2020 that appears similar to the attack on Defendant. As a result of this attack, Universal Health
3 Services suffered a four-week outage of its systems which caused as much as \$67 million in
4 recovery costs and lost revenue.⁸ Similarly, in 2021, Scripps Health suffered a cyberattack, an
5 event which effectively shut down critical health care services for a month and left numerous
6 patients unable to speak to their physicians or access vital medical and prescription records.⁹ A
7 few months later, University of San Diego Health suffered a similar attack.¹⁰

8 55. Due to the high-profile nature of these breaches, and other breaches of their kind,
9 Defendant was and/or certainly should have been on notice and aware of such attacks occurring in
10 the healthcare industry and, therefore, should have assumed and adequately performed the duty of
11 preparing for such an imminent attack. This is especially true given that Defendant is a large,
12 sophisticated operation with the resources to put adequate data security protocols in place.

13 56. Yet, despite the prevalence of public announcements of data breach and data
14 security compromises, Defendant failed to take appropriate steps to protect Representative
15 Plaintiff's and Class Members' PHI/PII and financial information from being compromised

16
17 **Defendant Had an Obligation to Protect the Stolen Information**

18 57. In addition to violating its purported commitment to its patients and community,
19 Defendant's failure to adequately secure Representative Plaintiff's and Class Members' sensitive
20 data also breaches duties it owes Representative Plaintiff and Class Members under statutory and
21 common law. Under HIPAA, healthcare providers have an affirmative duty to keep patients'
22 Protected Health Information private. As a covered entity, Defendant has a statutory duty under
23 HIPAA and other federal and state statutes to safeguard Representative Plaintiff's and Class
24 Members' data. Moreover, Representative Plaintiff and Class Members surrendered their highly

25
26 ⁸ <https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and> (last accessed November 5, 2021).

27 ⁹ <https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/> (last accessed November 5, 2021).

28 ¹⁰ <https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-accounts-impacted/2670302/> (last accessed November 5, 2021).

1 sensitive personal data to Defendant under the implied condition that Defendant would keep it
2 private and secure. Accordingly, Defendant also has an implied duty to safeguard their data,
3 independent of any statute.

4 58. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), they are required
5 to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E
6 (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule
7 (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R.
8 Part 160 and Part 164, Subparts A and C.

9 59. HIPAA’s Privacy Rule or Standards for Privacy of Individually Identifiable Health
10 Information establishes national standards for the protection of health information.

11 60. HIPAA’s Privacy Rule or Security Standards for the Protection of Electronic
12 Protected Health Information establishes a national set of security standards for protecting health
13 information that is kept or transferred in electronic form.

14 61. HIPAA requires Defendant to “comply with the applicable standards,
15 implementation specifications, and requirements” of HIPAA “with respect to electronic protected
16 health information.” 45 C.F.R. § 164.302.

17 62. “Electronic protected health information” is “individually identifiable health
18 information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45
19 C.F.R. § 160.103.

20 63. HIPAA’s Security Rule requires Defendant to do the following:
21 a. Ensure the confidentiality, integrity, and availability of all electronic protected
22 health information the covered entity or business associate creates, receives,
23 maintains, or transmits;
24 b. Protect against any reasonably anticipated threats or hazards to the security or
25 integrity of such information;
26 c. Protect against any reasonably anticipated uses or disclosures of such
27 information that are not permitted; and
28 d. Ensure compliance by its workforce.

64. HIPAA also requires Defendant to “review and modify the security measures
implemented ... as needed to continue provision of reasonable and appropriate protection of

1 | electronic protected health information” under 45 C.F.R. § 164.306(e), and to “[i]mplement
2 | technical policies and procedures for electronic information systems that maintain electronic
3 | protected health information to allow access only to those persons or software programs that have
4 | been granted access rights.” 45 C.F.R. § 164.312(a)(1).

5 | 65. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414,
6 | requires Defendant to provide notice of the Data Breach to each affected individual “without
7 | unreasonable delay and in no case later than 60 days following discovery of the breach.”

8 | 66. Defendant was also prohibited by the Federal Trade Commission Act (the “FTC
9 | Act”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting
10 | commerce.” The Federal Trade Commission (the “FTC”) has concluded that a company’s failure
11 | to maintain reasonable and appropriate data security for consumers’ sensitive personal information
12 | is an “unfair practice” in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*,
13 | 799 F.3d 236 (3d Cir. 2015).

14 | 67. In addition to its obligations under federal and state laws, Defendant owed a duty
15 | to Representative Plaintiff and Class Members to exercise reasonable care in obtaining, retaining,
16 | securing, safeguarding, deleting, and protecting the PHI/PII and financial information in
17 | Defendant’s possession from being compromised, lost, stolen, accessed, and misused by
18 | unauthorized persons. Defendant owed a duty to Representative Plaintiff and Class Members to
19 | provide reasonable security, including consistency with industry standards and requirements, and
20 | to ensure that its computer systems, networks, and protocols adequately protected the PHI/PII and
21 | financial information of Representative Plaintiff and Class Members.

22 | 68. Defendant owed a duty to Representative Plaintiff and Class Members to design,
23 | maintain, and test its computer systems, servers and networks to ensure that the PHI/PII and
24 | financial information in its possession was adequately secured and protected.

25 | 69. Defendant owed a duty to Representative Plaintiff and Class Members to create and
26 | implement reasonable data security practices and procedures to protect the PHI/PII and financial
27 | information in its possession, including not sharing information with other entities who maintained
28 | sub-standard data security systems.

1 70. Defendant owed a duty to Representative Plaintiff and Class Members to
2 implement processes that would immediately detect a breach on its data security systems in a
3 timely manner.

4 71. Defendant owed a duty to Representative Plaintiff and Class Members to act upon
5 data security warnings and alerts in a timely fashion.

6 72. Defendant owed a duty to Representative Plaintiff and Class Members to disclose
7 if its computer systems and data security practices were inadequate to safeguard individuals'
8 PHI/PII and/or financial information from theft because such an inadequacy would be a material
9 fact in the decision to entrust this PHI/PII and/or financial information to Defendant.

10 73. Defendant owed a duty of care to Representative Plaintiff and Class Members
11 because they were foreseeable and probable victims of any inadequate data security practices.

12 74. Defendant owed a duty to Representative Plaintiff and Class Members to encrypt
13 and/or more reliably encrypt Representative Plaintiff's and Class Members' PHI/PII and financial
14 information and monitor user behavior and activity in order to identify possible threats.

15
16 **Value of the Relevant Sensitive Information**

17 75. While the greater efficiency of electronic health records translates to cost savings
18 for providers, it also comes with the risk of privacy breaches. These electronic health records
19 contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's,
20 treatment plans) that is valuable to cyber criminals. One patient's complete record can be sold for
21 hundreds of dollars on the dark web. As such, PHI/PII and financial information are valuable
22 commodities for which a "cyber black market" exists in which criminals openly post stolen
23 payment card numbers, Social Security numbers, and other personal information on a number of
24 underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and
25 acutely affected by cyberattacks.

26 76. The high value of PHI/PII and financial information to criminals is further
27 evidenced by the prices they will pay through the dark web. Numerous sources cite dark web
28 pricing for stolen identity credentials. For example, personal information can be sold at a price

1 ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹¹ Experian reports
2 that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹² Criminals can
3 also purchase access to entire company data breaches from \$999 to \$4,995.¹³

4 77. Between 2005 and 2019, at least 249 million people were affected by health care
5 data breaches.¹⁴ Indeed, during 2019 alone, over 41 million healthcare records were exposed,
6 stolen, or unlawfully disclosed in 505 data breaches.¹⁵ In short, these sorts of data breaches are
7 increasingly common, especially among healthcare systems, which account for 30.03% of overall
8 health data breaches, according to cybersecurity firm Tenable.¹⁶

9 78. These criminal activities have and will result in devastating financial and personal
10 losses to Representative Plaintiff and Class Members. For example, it is believed that certain
11 PHI/PII compromised in the 2017 Experian data breach was being used, three years later, by
12 identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will
13 be an omnipresent threat for Representative Plaintiff and Class Members for the rest of their lives.
14 They will need to remain constantly vigilant.

15 79. The FTC defines identity theft as “a fraud committed or attempted using the
16 identifying information of another person without authority.” The FTC describes “identifying
17 information” as “any name or number that may be used, alone or in conjunction with any other
18 information, to identify a specific person,” including, among other things, “[n]ame, Social Security
19 number, date of birth, official State or government issued driver’s license or identification number,
20

21 ¹¹ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct.
22 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed July 28, 2021).

23 ¹² *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.
24 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 November 5, 2021).

25 ¹³ *In the Dark*, VPNOverview, 2019, available at:
<https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed November 5,
2021).

26 ¹⁴ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133> (last
accessed November 4, 2021).

27 ¹⁵ <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed
November 4, 2021).

28 ¹⁶ <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches> (last accessed November 4, 2021).

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

3 80. Identity thieves can use PHI/PII and financial information, such as that of
4 Representative Plaintiff and Class Members which Defendant failed to keep secure, to perpetrate
5 a variety of crimes that harm victims. For instance, identity thieves may commit various types of
6 government fraud such as immigration fraud, obtaining a driver’s license or identification card in
7 the victim’s name but with another’s picture, using the victim’s information to obtain government
8 benefits, or filing a fraudulent tax return using the victim’s information to obtain a fraudulent
9 refund.

10 81. The ramifications of Defendant’s failure to keep secure Representative Plaintiff’s
11 and Class Members’ PHI/PII and financial information are long lasting and severe. Once PHI/PII
12 and financial information is stolen, particularly identification numbers, fraudulent use of that
13 information and damage to victims may continue for years. Indeed, the PHI/PII and/or financial
14 information of Representative Plaintiff and Class Members was taken by hackers to engage in
15 identity theft or to sell it to other criminals who will purchase the PHI/PII and/or financial
16 information for that purpose. The fraudulent activity resulting from the Data Breach may not come
17 to light for years.

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

22 [L]aw enforcement officials told us that in some cases, stolen data may be held for
23 up to a year or more before being used to commit identity theft. Further, once stolen
24 data have been sold or posted on the Web, fraudulent use of that information may
25 continue for years. As a result, studies that attempt to measure the harm resulting
26 from data breaches cannot necessarily rule out all future harm.¹⁷

27
28 ¹⁷ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
<http://www.gao.gov/new.items/d07737.pdf> (last accessed November 4, 2021).

1 83. The harm to Representative Plaintiff and Class Members is especially acute given
2 the nature of the leaked data. Medical identity theft is one of the most common, most expensive,
3 and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, “medical-
4 related identity theft accounted for 43 percent of all identity thefts reported in the United States in
5 2013,” which is more than identity thefts involving banking and finance, the government and the
6 military, or education.¹⁸

7 84. “Medical identity theft is a growing and dangerous crime that leaves its victims
8 with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy
9 Forum. “Victims often experience financial repercussions and worse yet, they frequently discover
10 erroneous information has been added to their personal medical files due to the thief’s activities.”¹⁹

11 85. If cyber criminals manage to access financial information, health insurance
12 information and other personally sensitive data—as they did here—there is no limit to the amount
13 of fraud to which Defendant may expose Representative Plaintiff and Class Members.

14 86. A study by Experian found that the average total cost of medical identity theft is
15 “about \$20,000” per incident, and that a majority of victims of medical identity theft were forced
16 to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.²⁰ Almost
17 half of medical identity theft victims lose their healthcare coverage as a result of the incident, while
18 nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve
19 their identity theft at all.²¹

20 87. And data breaches are preventable.²² As Lucy Thompson wrote in the DATA
21 BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could

23 ¹⁸ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News,
24 Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/> (last accessed November 4, 2021).

¹⁹ *Id.*

²⁰ See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar. 3,
25 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last
26 accessed November 4, 2021).

²¹ *Id.*; see also Healthcare Data Breach: What to Know About them and What to Do After One,
27 EXPERIAN, [https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-
28 know-about-them-and-what-to-do-after-one/](https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/) (last accessed November 4, 2021).

²² Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in*
DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

1 have been prevented by proper planning and the correct design and implementation of appropriate
2 security solutions.”²³ She added that “[o]rganizations that collect, use, store, and share sensitive
3 personal data must accept responsibility for protecting the information and ensuring that it is not
4 compromised”²⁴

5 88. Most of the reported data breaches are a result of lax security and the failure to
6 create or enforce appropriate security policies, rules, and procedures . . . Appropriate information
7 security controls, including encryption, must be implemented and enforced in a rigorous and
8 disciplined manner so that a *data breach never occurs*.”²⁵

9 89. Here, Defendant knew of the importance of safeguarding PHI/PII and financial
10 information and of the foreseeable consequences that would occur if Representative Plaintiff’s and
11 Class Members’ PHI/PII and financial information was stolen, including the significant costs that
12 would be placed on Representative Plaintiff and Class Members as a result of a breach of this
13 magnitude. As detailed above, Defendant is a large, sophisticated organization with the resources
14 to deploy robust cybersecurity protocols. It knew, or should have known, that the development and
15 use of such protocols were necessary to fulfill its statutory and common law duties to
16 Representative Plaintiff and Class Members. Its failure to do so is, therefore, intentional, willful,
17 reckless and/or grossly negligent.

18 90. Defendant disregarded the rights of Representative Plaintiff and Class Members by,
19 *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and
20 reasonable measures to ensure that its network servers were protected against unauthorized
21 intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and
22 training practices in place to adequately safeguard Representative Plaintiff’s and Class Members’
23 PHI/PII and/or financial information; (iii) failing to take standard and reasonably available steps
24 to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an
25
26

27 ²³ *Id.* at 17.

28 ²⁴ *Id.* at 28.

²⁵ *Id.*

1 unreasonable duration of time; and (v) failing to provide Representative Plaintiff and Class
2 Members prompt and accurate notice of the Data Breach.

3
4 **FIRST CAUSE OF ACTION**
5 **Negligence**

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

8 92. At all times herein relevant, Defendant owed Representative Plaintiff and Class
9 Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII
10 and financial information and to use commercially reasonable methods to do so. Defendant took
11 on this obligation upon accepting and storing the PHI/PII and financial information of
12 Representative Plaintiff and Class Members in its computer systems and on its networks.

13 93. Among these duties, Defendant was expected:

- 14 a. to exercise reasonable care in obtaining, retaining, securing, safeguarding,
15 deleting and protecting the PHI/PII and financial information in its
16 possession;
- 17 b. to protect Representative Plaintiff's and Class Members' PHI/PII and
18 financial information using reasonable and adequate security procedures
19 and systems that were/are compliant with industry-standard practices;
- 20 c. to implement processes to quickly detect the Data Breach and to timely act
21 on warnings about data breaches; and
- 22 d. to promptly notify Representative Plaintiff and Class Members of any data
23 breach, security incident, or intrusion that affected or may have affected
24 their PHI/PII and financial information.

25 94. Defendant knew that the PHI/PII and financial information was private and
26 confidential and should be protected as private and confidential and, thus, Defendant owed a duty
27 of care not to subject Representative Plaintiff and Class Members to an unreasonable risk of harm
28 because they were foreseeable and probable victims of any inadequate security practices.

1 95. Defendant knew, or should have known, of the risks inherent in collecting and
2 storing PHI/PII and financial information, the vulnerabilities of its data security systems, and the
3 importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

4 96. Defendant knew, or should have known, that its data systems and networks did not
5 adequately safeguard Representative Plaintiff's and Class Members' PHI/PII and financial
6 information.

7 97. Only Defendant was in the position to ensure that its systems and protocols were
8 sufficient to protect the PHI/PII and financial information that Representative Plaintiff and Class
9 Members had entrusted to it.

10 98. Defendant breached its duties to Representative Plaintiff and Class Members by
11 failing to provide fair, reasonable, or adequate computer systems and data security practices to
12 safeguard the PHI/PII and financial information of Representative Plaintiff and Class Members.

13 99. Because Defendant knew that a breach of its systems could damage millions of
14 individuals, including Representative Plaintiff and Class Members, Defendant had a duty to
15 adequately protect its data systems and the PHI/PII and financial information contained thereon.

16 100. Representative Plaintiff's and Class Members' willingness to entrust Defendant
17 with their PHI/PII and financial information was predicated on the understanding that Defendant
18 would take adequate security precautions. Moreover, only Defendant had the ability to protect its
19 systems and the PHI/PII and financial information they stored on them from attack. Thus,
20 Defendant had a special relationship with Representative Plaintiff and Class Members.

21 101. Defendant also had independent duties under state and federal laws that required
22 Defendant to reasonably safeguard Representative Plaintiff's and Class Members' PHI/PII and
23 financial information and promptly notify them about the Data Breach. These "independent duties"
24 are untethered to any contract between Defendant and Representative Plaintiff and/or the
25 remaining Class Members.

26 102. Defendant breached its general duty of care to Representative Plaintiff and Class
27 Members in, but not necessarily limited to, the following ways:
28

- 1 a. by failing to provide fair, reasonable, or adequate computer systems and
- 2 data security practices to safeguard the PHI/PII and financial information of
- 3 Representative Plaintiff and Class Members;
- 4 b. by failing to timely and accurately disclose that Representative Plaintiff's
- 5 and Class Members' PHI/PII and financial information had been improperly
- 6 acquired or accessed;
- 7 c. by failing to adequately protect and safeguard the PHI/PII and financial
- 8 information by knowingly disregarding standard information security
- 9 principles, despite obvious risks, and by allowing unmonitored and
- 10 unrestricted access to unsecured PHI/PII and financial information;
- 11 d. by failing to provide adequate supervision and oversight of the PHI/PII and
- 12 financial information with which they were and are entrusted, in spite of the
- 13 known risk and foreseeable likelihood of breach and misuse, which
- 14 permitted an unknown third party to gather PHI/PII and financial
- 15 information of Representative Plaintiff and Class Members, misuse the
- 16 PHI/PII and intentionally disclose it to others without consent.
- 17 e. by failing to adequately train its employees to not store PHI/PII and
- 18 financial information longer than absolutely necessary;
- 19 f. by failing to consistently enforce security policies aimed at protecting
- 20 Representative Plaintiff's and the Class Members' PHI/PII and financial
- 21 information;
- 22 g. by failing to implement processes to quickly detect data breaches, security
- 23 incidents, or intrusions; and
- 24 h. by failing to encrypt Representative Plaintiff's and Class Members' PHI/PII
- 25 and financial information and monitor user behavior and activity in order to
- 26 identify possible threats.
- 27
- 28

19 103. Defendant's willful failure to abide by these duties was wrongful, reckless and
20 grossly negligent in light of the foreseeable risks and known threats.

21 104. As a proximate and foreseeable result of Defendant's grossly negligent conduct,
22 Representative Plaintiff and Class Members have suffered damages and are at imminent risk of
23 additional harms and damages (as alleged above).

24 105. The law further imposes an affirmative duty on Defendant to timely disclose the
25 unauthorized access and theft of the PHI/PII and financial information to Representative Plaintiff
26 and Class Members so that they could and/or still can take appropriate measures to mitigate
27 damages, protect against adverse consequences and thwart future misuse of their PHI/PII and
28 financial information.

1 106. Defendant breached its duty to notify Representative Plaintiff and Class Members
2 of the unauthorized access by waiting months after learning of the Data Breach to notify
3 Representative Plaintiff and Class Members and then by failing and continuing to fail to provide
4 Representative Plaintiff and Class Members sufficient information regarding the breach. To date,
5 Defendant has not provided sufficient information to Representative Plaintiff and Class Members
6 regarding the extent of the unauthorized access and continues to breach its disclosure obligations
7 to Representative Plaintiff and Class Members.

8 107. Further, through its failure to provide timely and clear notification of the Data
9 Breach to Representative Plaintiff and Class Members, Defendant prevented Representative
10 Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI/PII and
11 financial information, and to access their medical records and histories.

12 108. There is a close causal connection between Defendant's failure to implement
13 security measures to protect the PHI/PII and financial information of Representative Plaintiff and
14 Class Members and the harm suffered or risk of imminent harm suffered by Representative
15 Plaintiff and Class Members. Representative Plaintiff's and Class Members' PHI/PII and financial
16 information was accessed as the proximate result of Defendant's failure to exercise reasonable
17 care in safeguarding such PHI/PII and financial information by adopting, implementing, and
18 maintaining appropriate security measures.

19 109. Defendant's wrongful actions, inactions, and omissions constituted (and continue
20 to constitute) common law negligence.

21 110. The damages Representative Plaintiff and Class Members have suffered (as alleged
22 above) and will suffer were and are the direct and proximate result of Defendant's grossly
23 negligent conduct.

24 111. Additionally, 15 U.S.C. §45 (FTC Act, Section 5) prohibits "unfair . . . practices in
25 or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or
26 practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI/PII
27 and financial information. The FTC publications and orders described above also form part of the
28 basis of Defendant's duty in this regard.

1 112. Defendant violated 15 U.S.C. §45 by failing to use reasonable measures to protect
2 PHI/PII and financial information and not complying with applicable industry standards, as
3 described in detail herein. Defendant’s conduct was particularly unreasonable given the nature and
4 amount of PHI/PII and financial information it obtained and stored and the foreseeable
5 consequences of the immense damages that would result to Representative Plaintiff and Class
6 Members.

7 113. Defendant’s violation of 15 U.S.C. §45 constitutes negligence *per se*. Defendant
8 also violated the HIPAA Privacy and Security rules which, likewise, constitutes negligence *per se*.

9 114. As a direct and proximate result of Defendant’s negligence and negligence *per se*,
10 Representative Plaintiff and Class Members have suffered and will suffer injury, including but not
11 limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PHI/PII and financial
12 information is used; (iii) the compromise, publication, and/or theft of their PHI/PII and financial
13 information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery
14 from identity theft, tax fraud, and/or unauthorized use of their PHI/PII and financial information;
15 (v) lost opportunity costs associated with effort expended and the loss of productivity addressing
16 and attempting to mitigate the actual and future consequences of the Data Breach, including but
17 not limited to, efforts spent researching how to prevent, detect, contest, and recover from
18 embarrassment and identity theft; (vi) lost continuity in relation to their healthcare; (vii) the
19 continued risk to their PHI/PII and financial information, which may remain in Defendant’s
20 possession and is subject to further unauthorized disclosures so long as Defendant fails to
21 undertake appropriate and adequate measures to protect Representative Plaintiff’s and Class
22 Members’ PHI/PII and financial information in its continued possession; and (viii) future costs in
23 terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the
24 impact of the PHI/PII and financial information compromised as a result of the Data Breach for
25 the remainder of the lives of Representative Plaintiff and Class Members.

26 115. As a direct and proximate result of Defendant’s negligence and negligence *per se*,
27 Representative Plaintiff and Class Members have suffered and will continue to suffer other forms
28

1 of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy,
2 and other economic and non-economic losses.

3 116. Additionally, as a direct and proximate result of Defendant’s negligence and
4 negligence *per se*, Representative Plaintiff and Class Members have suffered and will suffer the
5 continued risks of exposure of their PHI/PII and financial information, which remain in
6 Defendant’s possession and are subject to further unauthorized disclosures so long as Defendant
7 fails to undertake appropriate and adequate measures to protect the PHI/PII and financial
8 information in its continued possession.

9
10 **SECOND CAUSE OF ACTION**
11 **Confidentiality of Medical Information Act**
12 **(Cal. Civ. Code §56, *et seq.*)**

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

15 118. Under California Civil Code §56.06, Defendant is deemed a “provider of
16 healthcare” and is, therefore, subject to the CMIA, California Civil Code §§ 56.10(a), (d) (e),
17 56.36(b), 56.101(a) and (b).

18 119. Under the CMIA, California Civil Code §56.05(k), Representative Plaintiff and
19 Class Members (except employees of Defendant whose records may have been accessed) are
20 deemed “patients.”

21 120. As defined in the CMIA, California Civil Code §56.05(j), Defendant disclosed
22 “medical information” to unauthorized persons without obtaining consent, in violation of
23 §56.10(a). Defendant’s misconduct, including failure to adequately detect, protect, and prevent
24 unauthorized disclosure, directly resulted in the unauthorized disclosure of Representative
25 Plaintiff’s and Class Members’ PHI/PII and financial information to unauthorized persons.

26 121. Defendant’s misconduct, including protecting and preserving the confidential
27 integrity of its clients’/customers’ PHI/PII and financial information, resulted in unauthorized
28 disclosure of sensitive and confidential PII that belongs to Representative Plaintiff and Class

1 Members to unauthorized persons, breaching the confidentiality of that information, thereby
2 violating California Civil Code §§ 56.06 and 56.101(a).

3 122. Because of Defendant's conduct, cybercriminals and/or other unauthorized
4 individuals viewed Representative Plaintiff's medical records.

5 123. Representative Plaintiff and Class Members have all been and continue to be
6 harmed as a direct, foreseeable and proximate result of Defendant's breach because Representative
7 Plaintiff and Class Members face, now and in the future, an imminent threat of identity theft, fraud
8 and for ransom demands. They must now spend time, effort and money to constantly monitor their
9 accounts and credit to surveille for any fraudulent activity.

10 124. Representative Plaintiff and Class Members were injured and have suffered
11 damages, as described above, from Defendant's illegal disclosure and negligent release of their
12 PHI/PII and financial information in violation of Cal. Civ. Code §§ 56.10 and 56.101 and,
13 therefore, seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal
14 statutory damages of \$1,000, punitive damages of \$3,000, injunctive relief, and attorneys' fees and
15 costs.

16
17 **THIRD CAUSE OF ACTION**
Invasion of Privacy

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

20 126. Representative Plaintiff and Class Members had a legitimate expectation of privacy
21 to their PHI/PII and financial information and were entitled to the protection of this information
22 against disclosure to unauthorized third-parties.

23 127. Defendant owed a duty to Representative Plaintiff and Class Members to keep their
24 PHI/PII and financial information confidential.

25 128. Defendant failed to protect and released to unknown and unauthorized third-parties
26 the PHI/PII and financial information of Representative Plaintiff and Class Members.

27
28

1 129. Defendant allowed unauthorized and unknown third-parties access to and
2 examination of the PHI/PII and financial information of Representative Plaintiff and Class
3 Members, by way of Defendant's failure to protect the PHI/PII and financial information.

4 130. The unauthorized release to, custody of, and examination by unauthorized third-
5 parties of the PHI/PII and financial information of Representative Plaintiff and Class Members is
6 highly offensive to a reasonable person.

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

14 132. The Data Breach constitutes an intentional interference with Representative
15 Plaintiff's and Class Members' interests in solitude or seclusion, either as to their persons or as to
16 their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

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

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

23 135. As a proximate result of the above acts and omissions of Defendant, the PHI/PII
24 and financial information of Representative Plaintiff and Class Members was disclosed to third-
25 parties without authorization, causing Representative Plaintiff and Class Members to suffer
26 damages.

27 136. Unless and until enjoined, and restrained by order of this Court, Defendant's
28 wrongful conduct will continue to cause great and irreparable injury to Representative Plaintiff

1 and Class Members in that the PHI/PII and financial information maintained by Defendant can be
2 viewed, distributed, and used by unauthorized persons for years to come. Representative Plaintiff
3 and Class Members have no adequate remedy at law for the injuries in that a judgment for
4 monetary damages will not end the invasion of privacy for Representative Plaintiff and/or Class
5 Members.

6
7 **FOURTH CAUSE OF ACTION**
8 **Breach of Confidence**

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

11 138. At all times during Representative Plaintiff's and Class Members' interactions with
12 Defendant, Defendant was fully aware of the confidential nature of the PHI/PII and financial
13 information that Representative Plaintiff and Class Members provided to them.

14 139. As alleged herein and above, Defendant's relationship with Representative Plaintiff
15 and the Class was governed by promises and expectations that Representative Plaintiff and Class
16 Members' PHI/PII and financial information would be collected, stored, and protected in
17 confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered
18 by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third-parties.

19 140. Representative Plaintiff and Class Members provided their respective PHI/PII and
20 financial information to Defendant with the explicit and implicit understandings that Defendant
21 would protect and not permit the PHI/PII and financial information to be accessed by, acquired by,
22 appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or
23 viewed by unauthorized third-parties.

24 141. Representative Plaintiff and Class Members also provided their PHI/PII and
25 financial information to Defendant with the explicit and implicit understanding that Defendant
26 would take precautions to protect their PHI/PII and financial information from unauthorized
27 access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or
28 viewing, such as following basic principles of protecting its networks and data systems.

1 142. Defendant voluntarily received, in confidence, Representative Plaintiff's and Class
2 Members' PHI/PII and financial information with the understanding that the PHI/PII and financial
3 information would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by,
4 exfiltrated by, released to, stolen by, used by and/or viewed by the public or any unauthorized
5 third-parties.

6 143. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from
7 occurring by, *inter alia*, not following best information security practices to secure Representative
8 Plaintiff's and Class Members' PHI/PII and financial information, Representative Plaintiff's and
9 Class Members' PHI/PII and financial information was accessed by, acquired by, appropriated by,
10 disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by
11 unauthorized third-parties beyond Representative Plaintiff's and Class Members' confidence, and
12 without their express permission.

13 144. As a direct and proximate cause of Defendant's actions and/or omissions,
14 Representative Plaintiff and Class Members have suffered damages, as alleged herein.

15 145. But for Defendant's failure to maintain and protect Representative Plaintiff's and
16 Class Members' PHI/PII and financial information in violation of the parties' understanding of
17 confidence, their PHI/PII and financial information would not have been accessed by, acquired by,
18 appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or
19 viewed by unauthorized third-parties. The Data Breach was the direct and legal cause of the misuse
20 of Representative Plaintiff's and Class Members' PHI/PII and financial information, as well as the
21 resulting damages.

22 146. The injury and harm Representative Plaintiff and Class Members suffered and will
23 continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of
24 Representative Plaintiff's and Class Members' PHI/PII and financial information. Defendant knew
25 its data systems and protocols for accepting and securing Representative Plaintiff's and Class
26 Members' PHI/PII and financial information had security and other vulnerabilities that placed
27 Representative Plaintiff's and Class Members' PHI/PII and financial information in jeopardy.
28

1 147. As a direct and proximate result of Defendant’s breaches of confidence,
2 Representative Plaintiff and Class Members have suffered and will suffer injury, as alleged herein,
3 including, but not limited to, (a) actual identity theft; (b) the compromise, publication, and/or theft
4 of their PHI/PII and financial information; (c) out-of-pocket expenses associated with the
5 prevention, detection, and recovery from identity theft and/or unauthorized use of their PHI/PII
6 and financial information; (d) lost opportunity costs associated with effort expended and the loss
7 of productivity addressing and attempting to mitigate the actual and future consequences of the
8 Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest,
9 and recover from identity theft; (e) the continued risk to their PHI/PII and financial information,
10 which remains in Defendant’s possession and is subject to further unauthorized disclosures so long
11 as Defendant fails to undertake appropriate and adequate measures to protect Class Members’
12 PHI/PII and financial information in their continued possession; (f) future costs in terms of time,
13 effort, and money that will be expended as result of the Data Breach for the remainder of the lives
14 of Representative Plaintiff and Class Members; (g) the diminished value of Representative
15 Plaintiff’s and Class Members’ PHI/PII and financial information; and (h) the diminished value of
16 Defendant’s services for which Representative Plaintiff and Class Members paid and received.

17
18 **FIFTH CAUSE OF ACTION**
Breach of Implied Contract

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

21 149. Through its course of conduct, Defendant, Representative Plaintiff and Class
22 Members entered into implied contracts for the Defendant to implement data security adequate to
23 safeguard and protect the privacy of Representative Plaintiff’s and Class Members’ PHI/PII and
24 financial information.

25 150. Defendant required Representative Plaintiff and Class Members to provide and
26 entrust their PHI/PII and financial information, including full names, birthdates and prescription
27 information and/or other financial information, as a condition of getting medical services, their
28 prescriptions and/or obtaining and maintain employment with Defendant.

1 151. Defendant solicited and invited Representative Plaintiff and Class Members to
2 provide their PHI/PII and financial information as part of Defendant's regular business practices.
3 Representative Plaintiff and Class Members accepted Defendant's offers and provided their
4 PHI/PII and financial information to Defendant.

5 152. As a condition of being direct customers/patients/employees of Defendant,
6 Representative Plaintiff and Class Members provided and entrusted their PHI/PII and financial
7 information to Defendant. In so doing, Representative Plaintiff and Class Members entered into
8 implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-
9 public information, to keep such information secure and confidential, and to timely and accurately
10 notify Representative Plaintiff and Class Members if their data had been breached and
11 compromised or stolen.

12 153. A meeting of the minds occurred when Representative Plaintiff and Class Members
13 agreed to, and did, provide their PHI/PII and financial information to Defendant, in exchange for,
14 amongst other things, the protection of their PHI/PII and financial information.

15 154. Representative Plaintiff and Class Members fully performed their obligations under
16 the implied contracts with Defendant.

17 155. Defendant breached the implied contracts it made with Representative Plaintiff and
18 Class Members by failing to safeguard and protect their PHI/PII and financial information and by
19 failing to provide timely and accurate notice to them that their PHI/PII and financial information
20 was compromised as a result of the Data Breach.

21 156. As a direct and proximate result of Defendant's above-described breach of implied
22 contract, Representative Plaintiff and Class Members have suffered (and will continue to suffer)
23 (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting
24 in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting
25 in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data;
26 (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other
27 economic and non-economic harm.

28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 17TH 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

**SIXTH CAUSE OF ACTION
Breach of the Implied Covenant of Good Faith and Fair Dealing**

157. 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.

158. Every contract in the State of California has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

159. Representative Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

160. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI/PII and financial information, failing to timely and accurately disclose the Data Breach to Representative Plaintiff and Class Members and continued acceptance of PHI/PII and financial 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.

161. Defendant acted in bad faith and/or with malicious motive in denying Representative Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

**SEVENTH CAUSE OF ACTION
Unfair Business Practices
(Cal. Bus. & Prof. Code, §17200, *et seq.*)**

162. 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.

163. Representative Plaintiff and Class Members further bring this cause of action, seeking equitable and statutory relief to stop the misconduct of Defendant, as complained of herein.

1 164. Defendant has engaged in unfair competition within the meaning of California
2 Business & Professions Code §§17200, *et seq.*, because Defendant’s conduct is unlawful, unfair
3 and/or fraudulent, as herein alleged.

4 165. Representative Plaintiff, the Class Members, and Defendant are each a “person” or
5 “persons” within the meaning of § 17201 of the California Unfair Competition Law (“UCL”).

6 166. The knowing conduct of Defendant, as alleged herein, constitutes an unlawful
7 and/or fraudulent business practice, as set forth in California Business & Professions Code
8 §§17200-17208. Specifically, Defendant conducted business activities while failing to comply
9 with the legal mandates cited herein, including HIPAA. Such violations include, but are not
10 necessarily limited to:

- 11 a. failure to maintain adequate computer systems and data security practices
12 to safeguard PHI/PII and financial information;
- 13 b. failure to disclose that its computer systems and data security practices were
14 inadequate to safeguard PHI/PII and financial information from theft;
- 15 c. failure to timely and accurately disclose the Data Breach to Representative
16 Plaintiff and Class Members;
- 17 d. continued acceptance of PHI/PII and financial information and storage of
18 other personal information after Defendant knew or should have known of
19 the security vulnerabilities of the systems that were exploited in the Data
20 Breach; and
- 21 e. continued acceptance of PHI/PII and financial information and storage of
22 other personal information after Defendant knew or should have known of
23 the Data Breach and before it allegedly remediated the Data Breach.

24 167. Defendant knew or should have known that its computer systems and data security
25 practices were inadequate to safeguard the PHI/PII and financial information of Representative
26 Plaintiff and Class Members, deter hackers and detect a breach within a reasonable time and that
27 the risk of a data breach was highly likely.

28 168. In engaging in these unlawful business practices, Defendant has enjoyed an
29 advantage over its competition and a resultant disadvantage to the public and Class Members.

30 169. Defendant’s knowing failure to adopt policies in accordance with and/or adhere to
31 these laws, all of which are binding upon and burdensome to Defendant’s competitors, engenders

1 an unfair competitive advantage for Defendant, thereby constituting an unfair business practice, as
2 set forth in California Business & Professions Code §§17200-17208.

3 170. Defendant has clearly established a policy of accepting a certain amount of
4 collateral damage, as represented by the damages to Representative Plaintiff and Class Members
5 herein alleged, as incidental to its business operations, rather than accept the alternative costs of
6 full compliance with fair, lawful and honest business practices ordinarily borne by responsible
7 competitors of Defendant and as set forth in legislation and the judicial record.

8 171. The UCL is, by its express terms, a cumulative remedy, such that remedies under its
9 provisions can be awarded in addition to those provided under separate statutory schemes and/or
10 common law remedies, such as those alleged in the other causes of action of this Complaint. *See*
11 Cal. Bus. & Prof. Code § 17205.

12 172. Representative Plaintiff and Class Members request that this Court enter such
13 orders or judgments as may be necessary to enjoin Defendant from continuing its unfair, unlawful,
14 and/or deceptive practices and to restore to Representative Plaintiff and Class Members any money
15 Defendant acquired by unfair competition, including restitution and/or equitable relief, including
16 disgorgement or ill-gotten gains, refunds of moneys, interest, reasonable attorneys' fees, and the
17 costs of prosecuting this class action, as well as any and all other relief that may be available at law
18 or equity.

19
20 **EIGHTH CAUSE OF ACTION**
Unjust Enrichment

21 173. 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.

23 174. By its wrongful acts and omissions described herein, Defendant has obtained a
24 benefit by unduly taking advantage of Representative Plaintiff and Class Members.

25 175. Defendant, prior to and at the time Representative Plaintiff and Class Members
26 entrusted their PHI/PII and financial information to Defendant for the purpose of obtaining health
27 services, caused Representative Plaintiff and Class Members to reasonably believe that Defendant
28 would keep such PHI/PII and financial information secure.

1 176. Defendant was aware, or should have been aware, that reasonable patients and
2 consumers would have wanted their PHI/PII and financial information kept secure and would not
3 have contracted with Defendant, directly or indirectly, had they know that Defendant's information
4 systems were sub-standard for that purpose.

5 177. Defendant was also aware that, if the substandard condition of and vulnerabilities
6 in its information systems were disclosed, it would negatively affect Representative Plaintiff's and
7 Class Members' decisions to seek health care services therefrom

8 178. Defendant failed to disclose facts pertaining to its substandard information systems,
9 defects and vulnerabilities therein before Representative Plaintiff and Class Members made their
10 decisions to make purchases, engage in commerce therewith, and seek health care services or
11 information. Instead, Defendant suppressed and concealed such information. By concealing and
12 suppressing that information, Defendant denied Representative Plaintiff and Class Members the
13 ability to make a rational and informed purchasing and health care decision and took undue
14 advantage of Representative Plaintiff and Class Members.

15 179. Defendant was unjustly enriched at the expense of Representative Plaintiff and
16 Class Members. Defendant received profits, benefits, and compensation, in part, at the expense of
17 Representative Plaintiff and Class Members. By contrast, Representative Plaintiff and Class
18 Members did not receive the benefit of their bargain because they paid for products and/or health
19 care services that did not satisfy the purposes for which they bought/sought them.

20 180. Since Defendant's profits, benefits, and other compensation were obtained by
21 improper means, Defendant is not legally or equitably entitled to retain any of the benefits,
22 compensation or profits it realized from these transactions.

23 181. Representative Plaintiff and Class Members seek an Order of this Court requiring
24 Defendant to refund, disgorge, and pay as restitution any profits, benefits and other compensation
25 obtained by Defendant from its wrongful conduct and/or the establishment of a constructive
26 trust from which Representative Plaintiff and Class Members may seek restitution.

27
28

RELIEF SOUGHT

WHEREFORE, Representative Plaintiff, on behalf of himself and each member of the proposed Class, respectfully requests that the Court enter judgment in his/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 the proposed class and/or any other appropriate subclasses under California Code of Civil Procedure § 382;

2. For an award of damages, including actual, nominal, consequential, statutory, and punitive 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 Plaintiff's and Class Members' PHI/PII and financial information, and from refusing to issue prompt, complete and accurate disclosures to Representative Plaintiff and Class Members;

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

- a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- 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 implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiff's and Class Members' PHI/PII and financial information;
- d. 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;
- e. prohibiting Defendant from maintaining Representative Plaintiff's and Class Members' PHI/PII and financial information on a cloud-based database;

COLE & VAN NOTE
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

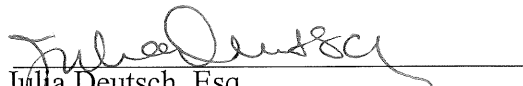
- f. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's networks are compromised, hackers cannot gain access to other portions of Defendant's systems;
 - g. requiring Defendant to conduct regular database scanning and securing checks;
 - h. 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 PHI/PII and financial information, as well as protecting the PHI/PII and financial information of Representative Plaintiff and Class Members;
 - i. 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 PHI/PII and financial information;
 - j. 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;
 - k. 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;
 - 8. For all other Orders, findings, and determinations sought in this Complaint.

JURY DEMAND

Representative Plaintiff, individually and on behalf of the Plaintiff Class, hereby demands a trial by jury for all issues triable by jury.

Dated: August 25, 2022

COLE & VAN NOTE

By: 
Julia Deutsch, Esq.
Attorneys for Representative Plaintiff
and the Plaintiff Class

COLE & VAN NOTE
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