

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 Scott Edward Cole, Esq. (S.B. #160744)
2 Laura Van Note, Esq. (S.B. #310160)
3 Colin Glenn Furlow, Esq. (S.B. #319219)
4 **COLE & VAN NOTE**
5 555 12th Street, Suite 2100
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: cgf@colevannote.com
12 Web: www.colevannote.com

13 Attorneys for Representative Plaintiff
14 and the Plaintiff Class

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

17 MICHELLE ROBERTSON, as parent for
18 minor child S.R., individually, and on
19 behalf of all others similarly situated,

20 Plaintiff,

21 v.

22 LA CLINICA DE LA RAZA, INC.

23 Defendant.

ELECTRONICALLY FILED
Superior Court of California,
County of Alameda
09/18/2023 at 03:41:57 PM
By: Milagros Cortez,
Deputy Clerk

Case No. **23CV044258**

CLASS ACTION

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

1. **NEGLIGENCE;**
2. **BREACH OF IMPLIED CONTRACT;**
3. **BREACH OF THE IMPLIED
COVENANT OF GOOD FAITH AND
FAIR DEALING;**
4. **VIOLATIONS OF THE CALIFORNIA
CONFIDENTIALITY OF MEDICAL
INFORMATION ACT (CAL. CIV.
CODE § 56, *ET SEQ.*);**
5. **VIOLATIONS OF CALIFORNIA'S
UNFAIR COMPETITION LAW (CAL.
BUS. & PROF. CODE § 17200, *ET
SEQ.*); AND**
6. **UNJUST ENRICHMENT**

[JURY TRIAL DEMANDED]

INTRODUCTION

1
2 1. Representative Plaintiff Michelle Robertson, on behalf of her minor child S.R.
3 (“Representative Plaintiff”) brings this class action against Defendant La Clinica de la Raza
4 (“Defendant” or “La Clinica”) for its failure to properly secure and safeguard Representative
5 Plaintiff’s and Class Members’ protected health information and personally identifiable
6 information stored within Defendant’s information network, including without limitation, names,
7 dates of birth, medical treatment information and health insurance information (these types of
8 information, *inter alia*, being thereafter referred to, collectively, as “protected health information”
9 or “PHI”¹ and “personally identifiable information” or “PII”).²

10 2. With this action, Representative Plaintiff seeks to hold Defendant responsible for
11 the harms it caused and will continue to cause Representative Plaintiff and at least 15,316 ³ other
12 similarly situated persons in the massive and preventable cyberattack purportedly discovered by
13 Defendant on February 8, 2023, by which cybercriminals infiltrated Defendant’s inadequately
14 protected employee email accounts and accessed highly sensitive PHI/PII which was being kept
15 unprotected (the “Data Breach”).

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

21
22 ¹ Protected health information (“PHI”) is a category of information that refers to an individual’s
23 medical records and history, which is protected under the Health Insurance Portability and
24 Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses,
25 personal or family medical histories and data points applied to a set of demographic information
26 for a particular patient.

27 ² Personally identifiable information (“PII”) generally incorporates information that can be
28 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 its 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, etc.).

³ “Breach Portal,” *U.S. Department of Health and Human Services Office for Civil Rights*,
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed September 15, 2023).

1 4. While Defendant claims to have discovered the breach as early as February 8, 2023,
2 Defendant did not begin informing victims of the Data Breach until September 1, 2023. Indeed,
3 Representative Plaintiff and Class Members were wholly unaware of the Data Breach until they
4 received letters from Defendant informing them of it. The Notice received by Representative
5 Plaintiff was dated September 1, 2023.

6 5. Defendant acquired, collected and stored Representative Plaintiff's and Class
7 Members' PHI/PII. Therefore, at all relevant times, Defendant knew or should have known that
8 Representative Plaintiff and Class Members would use Defendant's services to store and/or share
9 sensitive data, including highly confidential PHI/PII.

10 6. HIPAA establishes national minimum standards for the protection of individuals'
11 medical records and other protected health information. HIPAA generally applies to health plans
12 and insurers, healthcare clearinghouses and those healthcare providers that conduct certain
13 healthcare transactions electronically and sets minimum standards for Defendant's maintenance of
14 Representative Plaintiff's and Class Members' PHI/PII. More specifically, HIPAA requires
15 appropriate safeguards be maintained by organizations such as Defendant to protect the privacy of
16 protected health information and sets limits and conditions on the uses and disclosures that may
17 be made of such information without customer/patient authorization. HIPAA also establishes a
18 series of rights over Representative Plaintiff's and Class Members' PHI/PII, including rights to
19 examine and obtain copies of their health records and to request corrections thereto.

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

25 8. By obtaining, collecting, using and deriving a benefit from Representative
26 Plaintiff's and Class Members' PHI/PII, Defendant assumed legal and equitable duties to those
27 individuals. These duties arise from HIPAA and other state and federal statutes and regulations as
28 well as common law principles. Representative Plaintiff does not bring claims in this action for

1 direct violations of HIPAA, but charges Defendant with various legal violations merely predicated
2 upon the duties set forth in HIPAA.

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

14
15 **JURISDICTION AND VENUE**

16 10. This Court has jurisdiction over Representative Plaintiff's and Class Members'
17 claims for damages and injunctive relief pursuant to, *inter alia*, Cal. Civ. Code §56, *et seq.*
18 (Confidentiality of Medical Information Act), Cal. Civ. Code §1798, *et seq.* (Information Practices
19 Act of 1977) and Cal. Bus. & Prof. Code §17200, *et seq.*, among other California state statutes.

20 11. Venue as to Defendant is proper in this judicial district pursuant to California Code
21 of Civil Procedure § 395(a). Defendant is headquartered in and operates within this County and
22 transacts business, has agents, and is otherwise within this Court's jurisdiction for purposes of
23 service of process. The unlawful acts alleged herein have had a direct effect on Representative
24 Plaintiff and those similarly situated within the State of California and within this County.

25
26
27
28

PLAINTIFF

1
2 12. Representative Plaintiff is an adult individual and at all relevant times herein was a
3 resident and citizen of the State of California. Representative Plaintiff acts on behalf of her minor
4 daughter, S.R., who is a victim of the Data Breach.

5 13. Defendant received highly sensitive PHI/PII from Representative Plaintiff in
6 connection the services Representative Plaintiff received. As a result, Representative Plaintiff's
7 information was among the data accessed by an unauthorized third party in the Data Breach.

8 14. At all times herein relevant, Representative Plaintiff is and was a member of the
9 Class.

10 15. As required in order to obtain services from Defendant, Representative Plaintiff
11 provided Defendant with highly sensitive PHI/PII.

12 16. Representative Plaintiff's PHI/PII was exposed in the Data Breach because
13 Defendant stored Representative Plaintiff's PHI/PII. Representative Plaintiff's PHI/PII was within
14 the possession and control of Defendant at the time of the Data Breach.

15 17. Representative Plaintiff received a letter from Defendant, dated September 1, 2023,
16 stating Representative Plaintiff's PHI/PII was involved in the Data Breach (the "Notice").

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

23 19. Representative Plaintiff suffered actual injury in the form of damages to and
24 diminution in the value of Representative Plaintiff's PHI/PII—a form of intangible property that
25 Representative Plaintiff entrusted to Defendant, which was compromised in and as a result of the
26 Data Breach.

27 20. Representative Plaintiff suffered lost time, annoyance, interference and
28 inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss

1 of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling
2 Representative Plaintiff's PHI/PII.

3 21. Representative Plaintiff suffered imminent and impending injury arising from the
4 substantially increased risk of fraud, identity theft and misuse resulting from Representative
5 Plaintiff's PHI/PII, in combination with Representative Plaintiff's name, being placed in the hands
6 of unauthorized third parties/criminals.

7 22. Representative Plaintiff has a continuing interest in ensuring that Representative
8 Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendant's
9 possession, is protected and safeguarded from future breaches.

10
11 **DEFENDANT**

12 23. Defendant is a California nonprofit corporation with a principal place of business
13 located at 1450 Fruitvale Avenue, Suite J, Oakland, California 94601. Defendant provides multi-
14 lingual, accessible full-scope healthcare services in the East San Francisco Bay Area.⁴

15 24. The true names and capacities of persons or entities, whether individual, corporate,
16 associate or otherwise, who may be responsible for some of the claims alleged here are currently
17 unknown to Representative Plaintiff. Representative Plaintiff will seek leave of court to amend
18 this Complaint to reflect the true names and capacities of such responsible parties when their
19 identities become known.

20
21 **CLASS ACTION ALLEGATIONS**

22 25. Representative Plaintiff brings this action pursuant to the provisions of California
23 Code of Civil Procedure § 382, on behalf of Representative Plaintiff and the following class (the
24 "Class"):

25 "All individuals within the State of California whose PHI/PII was exposed
26 to unauthorized third parties as a result of the data breach discovered by
27 Defendant on February 8, 2023."

28 ⁴ "About," *La Clinica*, <https://laclinica.org/about> (last accessed September 15, 2023).

1 26. Excluded from the Class are the following individuals and/or entities: Defendant
2 and Defendant's parents, subsidiaries, affiliates, officers and directors and any entity in which
3 Defendant has a controlling interest, all individuals who make a timely election to be excluded
4 from this proceeding using the correct protocol for opting out, any and all federal, state or local
5 governments, including but not limited to its departments, agencies, divisions, bureaus, boards,
6 sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this
7 litigation, as well as their immediate family members.

8 27. In the alternative, Representative Plaintiff requests additional Subclasses as
9 necessary based on the types of PHI/PII that were compromised.

10 28. Representative Plaintiff reserves the right to amend the above definition or to
11 propose subclasses in subsequent pleadings and motions for class certification.

12 29. This action has been brought and may properly be maintained as a class action
13 under California Code of Civil Procedure § 382 because there is a well-defined community of
14 interest in the litigation and membership in the proposed Class is easily ascertainable.

15 a. Numerosity: A class action is the only available method for the fair
16 and efficient adjudication of this controversy. The members of the
17 Plaintiff Class are so numerous that joinder of all members is
18 impractical, if not impossible. Representative Plaintiff is informed
19 and believes and, on that basis alleges that the total number of Class
20 Members is at least 15,000 individuals. Membership in the Class
21 will be determined by analysis of Defendant's records.

22 b. Commonality: Representative Plaintiff and the Class Members
23 share a community of interest in that there are numerous common
24 questions and issues of fact and law which predominate over any
25 questions and issues solely affecting individual members, including
26 but not necessarily limited to:

- 27 1) Whether Defendant had a legal duty to Representative Plaintiff
28 and the Class to exercise due care in collecting, storing, using
 and/or safeguarding their PHI/PII;
- 2) Whether Defendant knew or should have known of the
 susceptibility of its data security systems to a data breach;
- 3) Whether Defendant's security procedures and practices to
 protect its systems were reasonable in light of the measures
 recommended by data security experts;
- 4) Whether Defendant's failure to implement adequate data
 security measures allowed the Data Breach to occur;

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

- 5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;
 - 6) Whether Defendant adequately, promptly and accurately informed Representative Plaintiff and Class Members that their PHI/PII had been compromised;
 - 7) How and when Defendant actually learned of the Data Breach;
 - 8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Representative Plaintiff's and Class Members' PHI/PII;
 - 9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
 - 10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiff's and Class Members' PHI/PII;
 - 11) 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
 - 12) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.
- c. Typicality: 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.
- d. Adequacy of Representation: Representative Plaintiff in this class action is an adequate representative of the Plaintiff Class in that the Representative Plaintiff has the same interest in the litigation of this case as the 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.
- e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct

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

alleged herein. 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 inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

30. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

31. 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 Representative Plaintiff.

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

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

1 **COMMON FACTUAL ALLEGATIONS**

2 **The Cyberattack**

3 34. In the course of the Data Breach, one or more unauthorized third parties accessed
4 Class Members' sensitive data, including but not limited to names, dates of birth, medical
5 treatment information, and health insurance information. Representative Plaintiff was among the
6 individuals whose data was accessed in the Data Breach.

7 35. According to the Data Breach Notification that Defendant filed with the U.S.
8 Department of Health and Human Services Office for Civil Rights, 15,316 persons were affected
9 by the Data Breach.⁵

10 36. Representative Plaintiff was provided the information detailed above upon
11 Representative Plaintiff's receipt of a letter from Defendant, dated September 1, 2023.
12 Representative Plaintiff was not aware of the Data Breach until receiving that letter.

13
14 **Defendant's Failed Response to the Breach**

15 37. Upon information and belief, the unauthorized third-party cybercriminals gained
16 access to Representative Plaintiff's and Class Members' PHI/PII with the intent of misusing the
17 PHI/PII, including marketing and selling Representative Plaintiff's and Class Members' PHI/PII.

18 38. Not until after roughly seven months after it claims to have discovered the Data
19 Breach did Defendant begin sending the Notice to persons whose PHI/PII Defendant confirmed
20 was potentially compromised as a result of the Data Breach. The Notice provided basic details of
21 the Data Breach and Defendant's recommended next steps.

22 39. The Notice included, *inter alia*, the claims that Defendant had learned of the Data
23 Breach on February 8, 2023, and Defendant later discovered the unauthorized access began as
24 early as January 24, 2023.

25 40. Defendant had and continues to have obligations created by HIPAA, applicable
26 federal and state law as set forth herein, reasonable industry standards, common law and its own

27
28 ⁵ "Breach Portal," *U.S. Department of Health and Human Services Office for Civil Rights*,
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed September 15, 2023).

1 assurances and representations to keep Representative Plaintiff's and Class Members' PHI/PII
2 confidential and to protect such PHI/PII from unauthorized access.

3 41. Representative Plaintiff and Class Members were required to provide their PHI/PII
4 to Defendant in order to receive services, and as part of providing services, Defendant created,
5 collected and stored Representative Plaintiff's and Class Members' PHI/PII with the reasonable
6 expectation and mutual understanding that Defendant would comply with its obligations to keep
7 such information confidential and secure from unauthorized access.

8 42. Despite this, Representative Plaintiff and the Class Members remain, even today,
9 in the dark regarding what particular data was stolen, the particular malware used and what steps
10 are being taken, if any, to secure their PHI/PII going forward. Representative Plaintiff and Class
11 Members are thus left to speculate as to where their PHI/PII ended up, who has used it and for
12 what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact
13 of the Data Breach and how exactly Defendant intends to enhance its information security systems
14 and monitoring capabilities so as to prevent further breaches.

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

20
21 **Defendant Collected/Stored Class Members' PHI/PII**

22 44. Defendant acquired, collected, stored and assured reasonable security over
23 Representative Plaintiff's and Class Members' PHI/PII.

24 45. As a condition of its relationships with Representative Plaintiff and Class Members,
25 Defendant required that Representative Plaintiff and Class Members entrust Defendant with highly
26 sensitive and confidential PHI/PII. Defendant, in turn, stored that information on Defendant's
27 system that was ultimately affected by the Data Breach.

28

1 46. By obtaining, collecting and storing Representative Plaintiff’s and Class Members’
2 PHI/PII, Defendant assumed legal and equitable duties over the PHI/PII and knew or should have
3 known that it was thereafter responsible for protecting Representative Plaintiff’s and Class
4 Members’ PHI/PII from unauthorized disclosure.

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

9 48. Defendant could have prevented the Data Breach, which began no later than
10 January 24, 2023, by properly securing and encrypting and/or more securely encrypting its servers
11 generally, as well as Representative Plaintiff’s and Class Members’ PHI/PII.

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

15 50. Due to the high-profile nature of these breaches, and other breaches of its kind,
16 Defendant was and/or certainly should have been on notice and aware of such attacks occurring in
17 its industry and, therefore, should have assumed and adequately performed the duty of preparing
18 for such an imminent attack. This is especially true given that Defendant is a large, sophisticated
19 operation with the resources to put adequate data security protocols in place.

20 51. And yet, despite the prevalence of public announcements of data breach and data
21 security compromises, Defendant failed to take appropriate steps to protect Representative
22 Plaintiff’s and Class Members’ PHI/PII from being compromised.

23
24 **Defendant Had an Obligation to Protect the Stolen Information**

25 52. In failing to adequately secure Representative Plaintiff’s and Class Members’
26 sensitive data, Defendant breached duties it owed Representative Plaintiff and Class Members
27 under statutory and common law. Under HIPAA, health insurance providers have an affirmative
28 duty to keep patients’ PHI secure. Similarly, as a covered entity, Defendant has a statutory duty

1 under HIPAA and other federal and state statutes to safeguard Representative Plaintiff's and Class
2 Members' PHI/PII. Moreover, Representative Plaintiff and Class Members surrendered their
3 highly sensitive PHI/PII to Defendant under the implied condition that Defendant would keep it
4 private and secure. Accordingly, Defendant also has an implied duty to safeguard their PHI/PII,
5 independent of any statute.

6 53. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to
7 comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E
8 ("Standards for Privacy of Individually Identifiable Health Information") and Security Rule
9 ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R.
10 Part 160 and Part 164, Subparts A and C.

11 54. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health
12 Information establishes national standards for the protection of health information.

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

16 56. HIPAA requires Defendant to "comply with the applicable standards,
17 implementation specifications, and requirements" of HIPAA "with respect to electronic protected
18 health information." 45 C.F.R. § 164.302.

19 57. "Electronic protected health information" is "individually identifiable health
20 information [...] that is (i) transmitted by electronic media; maintained in electronic media." 45
21 C.F.R. § 160.103.

22 58. HIPAA's Security Rule requires Defendant to do the following:

- 23 a. Ensure the confidentiality, integrity and availability of all electronic
24 protected health information the covered entity or business associate
creates, receives, maintains or transmits;
- 25 b. Protect against any reasonably anticipated threats or hazards to the
26 security or integrity of such information;
- 27 c. Protect against any reasonably anticipated uses or disclosures of such
28 information that are not permitted; and
- d. Ensure compliance by its workforce.

1 59. HIPAA also requires Defendant to “review and modify the security measures
2 implemented [...] as needed to continue provision of reasonable and appropriate protection of
3 electronic protected health information” under 45 C.F.R. § 164.306(e), and to “[i]mplement
4 technical policies and procedures for electronic information systems that maintain electronic
5 protected health information to allow access only to those persons or software programs that have
6 been granted access rights.” 45 C.F.R. § 164.312(a)(1).

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

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

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

24 63. Defendant owed a duty to Representative Plaintiff and Class Members to design,
25 maintain and test its computer systems, servers and networks to ensure that all PHI/PII in its
26 possession was adequately secured and protected.

27 64. Defendant owed a duty to Representative Plaintiff and Class Members to create and
28 implement reasonable data security practices and procedures to protect all PHI/PII in its

1 possession, including not sharing information with other entities who maintained sub-standard data
2 security systems.

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

6 66. Defendant owed a duty to Representative Plaintiff and Class Members to act upon
7 data security warnings and alerts in a timely fashion.

8 67. Defendant owed a duty to Representative Plaintiff and Class Members to disclose
9 if its computer systems and data security practices were inadequate to safeguard individuals'
10 PHI/PII from theft because such an inadequacy would be a material fact in the decision to entrust
11 their PHI/PII to Defendant.

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

14 69. Defendant owed a duty to Representative Plaintiff and Class Members to encrypt
15 and/or more reliably encrypt Representative Plaintiff's and Class Members' PHI/PII and monitor
16 user behavior and activity in order to identify possible threats.

17
18 **Value of the Relevant Sensitive Information**

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

27 71. The high value of PHI/PII to criminals is further evidenced by the prices they will
28 pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity

1 credentials. For example, personal information can be sold at a price ranging from \$40 to \$200,
2 and bank details have a price range of \$50 to \$200.⁶ Experian reports that a stolen credit or debit
3 card number can sell for \$5 to \$110 on the dark web.⁷ Criminals can also purchase access to entire
4 company data breaches from \$999 to \$4,995.⁸

5 72. Between 2005 and 2019, at least 249 million people were affected by healthcare
6 data breaches.⁹ Indeed, during 2019 alone, over 41 million healthcare records were exposed,
7 stolen, or unlawfully disclosed in 505 data breaches.¹⁰ In short, these sorts of data breaches are
8 increasingly common, especially among healthcare systems, which account for 30.03 percent of
9 overall health data breaches, according to cybersecurity firm Tenable.¹¹

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

16 74. The FTC defines identity theft as “a fraud committed or attempted using the
17 identifying information of another person without authority.” The FTC describes “identifying
18 information” as “any name or number that may be used, alone or in conjunction with any other
19

20 ⁶ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct.
21 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed September 15, 2023).

22 ⁷ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.
23 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 September 15, 2023).

24 ⁸ *In the Dark*, VPNOverview, 2019, available at:
25 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed September 15, 2023).

26 ⁹ *Healthcare Data Breaches: Insights and Implications*, Healthcare (Basel),
27 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133> (last
28 accessed September 15, 2023).

¹⁰ *December 2019 Healthcare Data Breach Report*, The HIPAA Journal,
<https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed
September 15, 2023).

¹¹ *Healthcare Security*, Tenable Blog, <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches> (last accessed September 15, 2023).

1 information, to identify a specific person,” including, among other things, “[n]ame, Social Security
2 number, date of birth, official State or government issued driver’s license or identification number,
3 alien registration number, government passport number, employer or taxpayer identification
4 number.”

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

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

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

20 [L]aw enforcement officials told us that in some cases, stolen data may be held for
21 up to a year or more before being used to commit identity theft. Further, once stolen
22 data have been sold or posted on the Web, fraudulent use of that information may
23 continue for years. As a result, studies that attempt to measure the harm resulting
24 from data breaches cannot necessarily rule out all future harm.¹²

25 78. The harm to Representative Plaintiff and Class Members is especially acute given
26 the nature of the leaked data. Medical identity theft is one of the most common, most expensive
27 and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, “medical-

28 ¹² *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
<http://www.gao.gov/new.items/d07737.pdf> (last accessed September 15, 2023).

1 related identity theft accounted for 43 percent of all identity thefts reported in the United States in
2 2013,” which is more than identity thefts involving banking and finance, the government and the
3 military, or education.¹³

4 79. “Medical identity theft is a growing and dangerous crime that leaves its victims
5 with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy
6 Forum. “Victims often experience financial repercussions and worse yet, they frequently discover
7 erroneous information has been added to their personal medical files due to the thief’s activities.”¹⁴

8 80. When cybercriminals access financial information, health insurance information
9 and other personally sensitive data—as they did here—there is no limit to the amount of fraud to
10 which Defendant may have exposed Representative Plaintiff and Class Members.

11 81. A study by Experian found that the average total cost of medical identity theft is
12 “about \$20,000” per incident, and that a majority of victims of medical identity theft were forced
13 to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.¹⁵ Almost
14 half of medical identity theft victims lose their healthcare coverage as a result of the incident, while
15 nearly one-third saw their insurance premiums rise, and 40 percent were never able to resolve their
16 identity theft at all.¹⁶

17 82. And data breaches are preventable.¹⁷ As Lucy Thompson wrote in the DATA
18 BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could
19 have been prevented by proper planning and the correct design and implementation of appropriate
20 security solutions.”¹⁸ She added that “[o]rganizations that collect, use, store, and share sensitive
21

22
23 ¹³ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News,
Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/> (last accessed September 15, 2023).

24 ¹⁴ *Id.*

25 ¹⁵ See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar. 3,
2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last
accessed September 15, 2023).

26 ¹⁶ *Id.*; see also Healthcare Data Breach: What to Know About them and What to Do After One,
EXPERIAN, [https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-
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 September 15, 2023).

27 ¹⁷ Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in*
DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

28 ¹⁸ *Id.* at 17.

1 personal data must accept responsibility for protecting the information and ensuring that it is not
2 compromised....”¹⁹

3 83. Most of the reported data breaches are a result of lax security and the failure to
4 create or enforce appropriate security policies, rules and procedures. Appropriate information
5 security controls, including encryption, must be implemented and enforced in a rigorous and
6 disciplined manner so that a *data breach never occurs*.²⁰

7 84. Here, Defendant knew of the importance of safeguarding PHI/PII and of the
8 foreseeable consequences that would occur if Representative Plaintiff’s and Class Members’
9 PHI/PII was stolen, including the significant costs that would be placed on Representative Plaintiff
10 and Class Members as a result of a breach of this magnitude. As detailed above, Defendant knew
11 or should have known that the development and use of such protocols were necessary to fulfill its
12 statutory and common law duties to Representative Plaintiff and Class Members. Its failure to do
13 so is therefore intentional, willful, reckless and/or grossly negligent.

14 85. Defendant disregarded the rights of Representative Plaintiff and Class Members by,
15 *inter alia*, (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and
16 reasonable measures to ensure that its network servers were protected against unauthorized
17 intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and
18 training practices in place to adequately safeguard Representative Plaintiff’s and Class Members’
19 PHI/PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach,
20 (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time,
21 and (v) failing to provide Representative Plaintiff and Class Members prompt and accurate notice
22 of the Data Breach.

23
24
25
26
27
28 ¹⁹ *Id.* at 28.

²⁰ *Id.*

1 **FIRST CAUSE OF ACTION**

2 **Negligence**

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

5 87. At all times herein relevant, Defendant owed Representative Plaintiff and Class
6 Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII
7 and to use commercially reasonable methods to do so. Defendant took on this obligation upon
8 accepting and storing Representative Plaintiff's and Class Members' PHI/PII on its computer
9 systems and networks.

10 88. Among these duties, Defendant was expected:

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

21 89. Defendant knew that the PHI/PII was private and confidential and should be
22 protected as private and confidential and, thus, Defendant owed a duty of care not to subject
23 Representative Plaintiff and Class Members to an unreasonable risk of harm because they were
24 foreseeable and probable victims of any inadequate security practices.

25 90. Defendant knew or should have known of the risks inherent in collecting and
26 storing PHI/PII, the vulnerabilities of its data security systems and the importance of adequate
27 security. Defendant knew about numerous, well-publicized data breaches.

28 91. Defendant knew or should have known that its data systems and networks did not
adequately safeguard Representative Plaintiff's and Class Members' PHI/PII.

1 92. Only Defendant was in the position to ensure that its systems and protocols were
2 sufficient to protect the PHI/PII that Representative Plaintiff and Class Members had entrusted to
3 it.

4 93. Defendant breached its duties to Representative Plaintiff and Class Members by
5 failing to provide fair, reasonable or adequate computer systems and data security practices to
6 safeguard Representative Plaintiff's and Class Members' PHI/PII.

7 94. Because Defendant knew that a breach of its systems could damage thousands of
8 individuals, including Representative Plaintiff and Class Members, Defendant had a duty to
9 adequately protect its data systems and the PHI/PII contained thereon.

10 95. Representative Plaintiff's and Class Members' willingness to entrust Defendant
11 with its PHI/PII was predicated on the understanding that Defendant would take adequate security
12 precautions. Moreover, only Defendant had the ability to protect its systems and the PHI/PII it
13 stored on them from attack. Thus, Defendant had a special relationship with Representative
14 Plaintiff and Class Members.

15 96. Defendant also had independent duties under state and federal laws that required
16 Defendant to reasonably safeguard Representative Plaintiff's and Class Members' PHI/PII and
17 promptly notify them about the Data Breach. These "independent duties" are untethered to any
18 contract between Defendant and Representative Plaintiff and/or the remaining Class Members.

19 97. Defendant breached its general duty of care to Representative Plaintiff and Class
20 Members in, but not necessarily limited to, the following ways:

- 21 a. by failing to provide fair, reasonable, or adequate computer systems
22 and data security practices to safeguard Representative Plaintiff's
23 and Class Members' PHI/PII;
- 24 b. by failing to timely and accurately disclose that Representative
25 Plaintiff's and Class Members' PHI/PII had been improperly
26 acquired or accessed;
- 27 c. by failing to adequately protect and safeguard the PHI/PII by
28 knowingly disregarding standard information security principles,
 despite obvious risks, and by allowing unmonitored and unrestricted
 access to unsecured PHI/PII;
- d. by failing to provide adequate supervision and oversight of the
 PHI/PII with which it was and is entrusted, in spite of the known

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

risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Representative Plaintiff's and Class Members' PHI/PII, misuse the PHI/PII and intentionally disclose it to others without consent;

- e. by failing to adequately train its employees to not store PHI/PII longer than absolutely necessary;
- f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff's and the Class Members' PHI/PII;
- g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and
- h. by failing to encrypt Representative Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

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

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

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

101. Defendant breached its duty to notify Representative Plaintiff and Class Members of the unauthorized access by waiting almost a year after learning of the Data Breach to notify Representative Plaintiff and Class Members and then by failing and continuing to fail to provide Representative Plaintiff and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiff and Class Members.

102. Further, through its failure to provide timely and clear notification of the Data Breach to Representative Plaintiff and Class Members, Defendant prevented Representative

1 Plaintiff and Class Members from taking meaningful, proactive steps to, *inter alia*, secure and/or
2 access their PHI/PII.

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

9 104. Defendant’s wrongful actions, inactions and omissions constituted (and continue to
10 constitute) common law negligence.

11 105. The damages Representative Plaintiff and Class Members have suffered (as alleged
12 above) and will continue to suffer were and are the direct and proximate result of Defendant’s
13 grossly negligent conduct.

14 106. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits “unfair [...] practices
15 in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or
16 practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI/PII.
17 The FTC publications and orders described above also form part of the basis of Defendant’s duty
18 in this regard.

19 107. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect
20 PHI/PII and not complying with applicable industry standards, as described in detail herein.
21 Defendant’s conduct was particularly unreasonable given the nature and amount of PHI/PII it
22 obtained and stored and the foreseeable consequences of the immense damages that would result
23 to Representative Plaintiff and Class Members.

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

26 109. 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 injury,
28 including but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their

1 PHI/PII is used, (iii) the compromise, publication and/or theft of their PHI/PII, (iv) out-of-pocket
2 expenses associated with the prevention, detection and recovery from identity theft, tax fraud
3 and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with effort expended
4 and the loss of productivity addressing and attempting to mitigate the actual and future
5 consequences of the Data Breach, including but not limited to efforts spent researching how to
6 prevent, detect, contest and recover from embarrassment and identity theft, (vi) lost continuity in
7 relation to their personal records, (vii) the continued risk to their PHI/PII, which may remain in
8 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant
9 fails to undertake appropriate and adequate measures to protect Representative Plaintiff's and
10 Class Members' PHI/PII in its continued possession, and (viii) future costs in terms of time, effort
11 and money that will be expended to prevent, detect, contest and repair the impact of the PHI/PII
12 compromised as a result of the Data Breach for the remainder of the lives of Representative
13 Plaintiff and Class Members.

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

18 111. Additionally, as a direct and proximate result of Defendant's negligence and
19 negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to
20 suffer the continued risks of exposure of their PHI/PII, which remains in Defendant's possession
21 and is subject to further unauthorized disclosures so long as Defendant fails to undertake
22 appropriate and adequate measures to protect PHI/PII in its continued possession.
23
24
25
26
27
28

SECOND CAUSE OF ACTION
Breach of Implied Contract

112. 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.

113. Through their course of conduct, Defendant, Representative Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiff's and Class Members' PHI/PII.

114. Defendant required Representative Plaintiff and Class Members to provide and entrust their PHI/PII as a condition of obtaining Defendant's goods/services/employment from/with Defendant.

115. Defendant solicited and invited Representative Plaintiff and Class Members to provide their PHI/PII as part of Defendant's regular business practices. Representative Plaintiff and Class Members accepted Defendant's offers and provided their PHI/PII to Defendant.

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

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

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

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

1 **FOURTH CAUSE OF ACTION**
2 **California Confidentiality of Medical Information Act**
3 **Cal. Civ. Code § 56, et seq.**

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

6 127. Under California Civil Code § 56.06, Defendant is deemed a “provider of
7 healthcare, healthcare service plan or contractor” and is, therefore, subject to the CMIA, California
8 Civil Code §§ 56.10(a), (d) (e), 56.36(b), 56.101(a) and (b).

9 128. Under the CMIA, California Civil Code §56.05(k), Representative Plaintiff and
10 Class Members are deemed “patients.”

11 129. As defined in the CMIA, California Civil Code § 56.05(j), Defendant disclosed
12 “medical information” to unauthorized persons without obtaining consent, in violation of §
13 56.10(a). Defendant’s misconduct, including failure to adequately detect, protect and prevent
14 unauthorized disclosure, directly resulted in the unauthorized disclosure of Representative
15 Plaintiff’s and Class Members’ PHI/PII and financial information to unauthorized persons.

16 130. Defendant’s misconduct, including protecting and preserving the confidential
17 integrity of its patients’ PHI/PII and financial information, resulted in unauthorized disclosure of
18 sensitive and confidential information that belongs to Representative Plaintiff and Class Members
19 to unauthorized persons, breaching the confidentiality of that information, thereby violating
20 California Civil Code §§ 56.06 and 56.101(a).

21 131. As a result of the Data Breach, unauthorized third parties viewed Representative
22 Plaintiff(s)’ and Class Members’ protected medical information.

23 132. Representative Plaintiff and Class Members have all been and continue to be
24 harmed as a direct, foreseeable and proximate result of Defendant’s breach because Representative
25 Plaintiff and Class Members face, now and in the future, an imminent threat of identity theft, fraud
26 and for ransom demands. They must now spend time, effort and money to constantly monitor their
27 accounts and credit to surveil for any fraudulent activity.

28 133. Representative Plaintiff and Class Members were injured and have suffered
damages, as described above, from Defendant’s illegal disclosure and negligent release of their

1 PHI/PII and financial information in violation of Cal. Civ. Code §§ 56.10 and 56.101 and,
2 therefore, seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal
3 statutory damages of \$1,000, punitive damages of \$3,000, injunctive relief and attorneys' fees and
4 costs.

5
6 **FIFTH CAUSE OF ACTION**
7 **California Unfair Competition Law**
8 **Cal. Bus. & Prof. Code §§ 17200, *et seq.***

9 134. 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

11 135. Defendant is a "person" as defined by Cal. Bus. & Prof. Code §17201.

12 136. Defendant violated Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL") by engaging
13 in unlawful, unfair and deceptive business acts and practices.

14 137. Defendant's "unfair" acts and practices include:

- 15 a. Defendant failed to implement and maintain reasonable security
16 measures to protect Plaintiff's and Class Members' PHI/PII from
17 unauthorized disclosure, release, data breaches and theft, which was
18 a direct and proximate cause of the Data Breach. Defendant failed
19 to identify foreseeable security risks, remediate identified security
20 risks and adequately maintain and/or improve security following
21 previous cybersecurity incidents. This conduct, with little if any
22 utility, is unfair when weighed against the harm to Plaintiff and the
23 Class, whose PHI/PII has been compromised.
- 24 b. Defendant's failure to implement and maintain reasonable security
25 measures also was contrary to legislatively declared public policy
26 that seeks to protect consumers' data and ensure that entities that are
27 trusted with it use appropriate security measures. These policies are
28 reflected in laws, including the FTC Act (15 U.S.C. § 45, *et seq.*)
and California's Consumer Records Act (Cal. Civ. Code §
1798.81.5).
- c. Defendant's failure to implement and maintain reasonable security
measures also leads to substantial consumer injuries, as described
above, that are not outweighed by any countervailing benefits to
consumers or competition. Moreover, because consumers could not
know of Defendant's inadequate security, consumers could not have
reasonably avoided the harms that Defendant caused.
- d. Engaging in unlawful business practices by violating Cal. Civ. Code
§ 1798.82.

1 138. Defendant has engaged in “unlawful” business practices by violating multiple laws,
2 including California’s Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable
3 data security measures) and 1798.82 (requiring timely breach notification), California’s
4 Consumers Legal Remedies Act, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, *et*
5 *seq.*, and California common law.

6 139. Defendant’s unlawful, unfair and deceptive acts and practices include:

- 7 a. Failing to implement and maintain reasonable security and privacy
8 measures to protect Plaintiff’s and Class Members’ PHI/PII, which
9 was a direct and proximate cause of the Data Breach;
- 10 b. Failing to identify foreseeable security and privacy risks, remediate
11 identified security and privacy risks and adequately maintain and/or
12 improve security and privacy measures, which was a direct and
13 proximate cause of the Data Breach;
- 14 c. Failing to comply with common law and statutory duties pertaining
15 to the security and privacy of Plaintiff’s and Class Members’
16 PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45,
17 *et seq.*, and California’s Customer Records Act, Cal. Civ. Code §
18 1798.80, *et seq.*, which was a direct and proximate cause of the Data
19 Breach;
- 20 d. Misrepresenting that it would protect the privacy and confidentiality
21 of Plaintiff’s and Class Members’ PHI/PII, including by
22 implementing and maintaining reasonable security measures;
- 23 e. Misrepresenting that it would comply with common law and
24 statutory duties pertaining to the security and privacy of Plaintiff’s
25 and Class Members’ PHI/PII, including duties imposed by the FTC
26 Act, 15 U.S.C. § 45, *et seq.*, and California’s Customer Records Act,
27 Cal. Civ. Code § 1798.80, *et seq.*;
- 28 f. Omitting, suppressing and concealing the material fact that it did not
reasonably or adequately secure Plaintiff’s and Class Members’
PHI/PII; and
- g. Omitting, suppressing and concealing the material fact that it did not
comply with common law and statutory duties pertaining to the
security and privacy of Plaintiff’s and Class Members’ PHI/PII,
including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*,
and California’s Customer Records Act, Cal. Civ. Code §§ 1798.80,
et seq.

138. Defendant’s representations and omissions were material because they were likely
to deceive reasonable consumers about the adequacy of Defendant’s data security and ability to
protect the confidentiality of consumers’ PHI/PII.

1 148. Defendant was also aware that if the substandard condition of and vulnerabilities
2 in their information systems were disclosed, it would negatively affect Representative Plaintiff's
3 and Class Members' decisions to engage with Defendant.

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

11 150. Defendant was unjustly enriched at the expense of Representative Plaintiff and
12 Class Members. Defendant received profits, benefits, and compensation, in part, at the expense of
13 Representative Plaintiff and Class Members. By contrast, Representative Plaintiff and Class
14 Members did not receive the benefit of their bargain because they paid for services that did not
15 satisfy the purposes for which they bought/sought them.

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

19 152. Representative Plaintiff and Class Members seek an Order of this Court requiring
20 Defendant to refund, disgorge, and pay as restitution any profits, benefits and other compensation
21 obtained by Defendant from their wrongful conduct and/or the establishment of a constructive
22 trust from which Representative Plaintiff and Class Members may seek restitution.

23
24
25
26
27
28

RELIEF SOUGHT

1
2 **WHEREFORE**, Representative Plaintiff, on Representative Plaintiff's own behalf and on
3 behalf of each member of the proposed Class, respectfully requests that the Court enter judgment
4 in Representative Plaintiff's favor and for the following specific relief against Defendant as
5 follows:

6 1. That the Court declare, adjudge and decree that this action is a proper class action
7 and certify each of the proposed Class under California Code of Civil Procedure § 382, including
8 appointment of Representative Plaintiff's counsel as Class Counsel;

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

11 3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful
12 activities;

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

15 5. For equitable relief enjoining Defendant from engaging in the wrongful conduct
16 complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiff's and
17 Class Members' PHI/PII, and from refusing to issue prompt, complete and accurate disclosures to
18 Representative Plaintiff and Class Members;

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

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

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

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

- d. 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;
 - e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis;
 - f. prohibiting Defendant from maintaining Representative Plaintiff's and Class Members' PHI/PII on a cloud-based database;
 - g. requiring Defendant to segment data by creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
 - h. requiring Defendant to conduct regular database scanning and securing checks;
 - i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Representative Plaintiff and Class Members;
 - j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personal identifying information;
 - k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated;
 - l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.
7. For prejudgment interest on all amounts awarded, at the prevailing legal rate;
8. For an award of attorneys' fees, costs and litigation expenses, as allowed by law;

and

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


9. For all other Orders, findings and determinations identified and 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: September 18, 2023

COLE & VAN NOTE

By: 

Laura Van Note, Esq.
Attorneys for Representative Plaintiff and the Plaintiff Class

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800