

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 **COLE & VAN NOTE**
4 555 12th Street, Suite 2100
5 Oakland, California 94607
6 Telephone: (510) 891-9800
7 Facsimile: (510) 891-7030
8 Email: sec@colevannote.com
9 Email: lvn@colevannote.com
10 Web: www.colevannote.com

11 Attorneys for Representative Plaintiff

12 **IN THE SUPERIOR COURT OF THE STATE OF CALIFORNIA**
13 **IN AND FOR THE COUNTY OF VENTURA**

14 VERONICA HUBBARD, individually, and
15 on behalf of all others similarly situated,

16 Plaintiff,

17 vs.

18 LIVINGSTON MEMORIAL VNA
19 HEALTH CORP., LIVINGSTON
20 MEMORIAL VISITING NURSE
21 ASSOCIATION, LIVINGSTON
22 CAREGIVERS, and DOES 1 through 100,
23 inclusive,

24 Defendants.

Case No. 56-2023-00576342-CU-NP

CLASS ACTION

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

1. NEGLIGENCE;
2. BREACH OF IMPLIED CONTRACT;
3. CONFIDENTIALITY OF MEDICAL INFORMATION ACT (CAL. CIV. CODE § 56);

[JURY TRIAL DEMANDED]

1 Representative Plaintiff alleges as follows:
2

3 **INTRODUCTION**

4 1. Representative Plaintiff Veronica Hubbard (“Representative Plaintiff”) brings this
5 class action against Defendants Livingston Memorial VNA Health Corp., Livingston Memorial
6 Visiting Nurse Association, Livingston Caregivers and Does 1-100 (collectively “Defendants”)
7 for their failure to properly secure and safeguard Class Members’ protected health information and
8 personally identifiable information stored within Defendants’ information network, including,
9 without limitation, HIC Numbers, dates of birth, medical conditions, medical reference numbers,
10 demographic information, private health insurance providers and private health plan numbers
11 (these types of information, *inter alia*, being thereafter referred to, collectively, as “protected
12 health information” or “PHI”¹ and “personally identifiable information” or “PII”).²

13 2. With this action, Representative Plaintiff seeks to hold Defendants responsible for
14 the harms they caused and will continue to cause Representative Plaintiff and countless other
15 similarly situated persons in the massive and preventable cyberattack purportedly discovered by
16 Defendants on February 19, 2022 by which cybercriminals infiltrated Defendants’ inadequately
17 protected network servers and accessed highly sensitive PHI/PII belonging to both adults and
18 children, which was being kept unprotected (the “Data Breach”).

19 3. Representative Plaintiff further seeks to hold Defendants responsible for not
20 ensuring that her PHI/PII was maintained in a manner consistent with industry, the Health
21 Insurance Portability and Accountability Act of 1996 (“HIPAA”) Privacy Rule (45 CFR, Part 160

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 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).

1 and Parts A and E of Part 164), the HIPAA Security Rule (45 CFR Part 160 and Subparts A and
2 C of Part 164), and other relevant standards.

3 4. While Defendants claim to have discovered the breach as early as February 19,
4 2022, Defendants did not begin informing victims of the Data Breach until January 2023 and failed
5 to inform victims when or for how long the Data Breach occurred. Indeed, Representative Plaintiff
6 and Class Members were wholly unaware of the Data Breach until they received letters from
7 Defendants informing them of it. The notice received by Representative Plaintiff was dated
8 January 20, 2023.

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

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

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

28

1 and within this County.
2

3 **PLAINTIFF**

4 12. Representative Plaintiff is an adult individual and, at all relevant times herein, a
5 resident and citizen of California. Representative Plaintiff is a victim of the Data Breach.

6 13. Defendants received highly sensitive personal and medical information from
7 Representative Plaintiff in connection with the home health services she received from Defendants.
8 As a result, Representative Plaintiff's information was among the data accessed by an unauthorized
9 third party in the Data Breach.

10 14. Representative Plaintiff received—and was a “consumer” for purposes of obtaining
11 services from Defendants within California.

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

14 16. As required in order to obtain services from Defendant, Representative Plaintiff
15 provided Defendants with highly sensitive personal, health and insurance information.

16 17. Representative Plaintiff's PHI/PII was exposed in the Data Breach because
17 Defendants stored and/or shared Representative Plaintiff's PHI/PII. Representative Plaintiff's
18 PHI/PII was within the possession and control of Defendants at the time of the Data Breach.

19 18. Representative Plaintiff received a letter from Defendant, dated on or about January
20 20, 2023, stating that Representative Plaintiff's PHI/PII was involved in the Data Breach (the
21 “Notice”).

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

27 20. Additionally, Plaintiff began receiving spam emails related to her medical
28 condition after the Data Breach. Plaintiff has lost time remediating these spam emails. Upon

1 information and belief, Plaintiff believes that these spam emails are occurring as a result of the
2 Data Breach as they directly relate to her medical condition.

3 21. Representative Plaintiff suffered actual injury in the form of damages to and
4 diminution in the value of Representative Plaintiff's PHI/PII—a form of intangible property that
5 Representative Plaintiff entrusted to Defendant, which was compromised in and as a result of the
6 Data Breach.

7 22. Representative Plaintiff suffered lost time, annoyance, interference, and
8 inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss
9 of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling
10 Representative Plaintiff's PHI/PII. In particular, Plaintiff has anxiety over private photographs of
11 her medical condition taken by Livingston Memorial being released.

12 23. Representative Plaintiff has suffered imminent and impending injury arising from
13 the substantially increased risk of fraud, identity theft and misuse resulting from Representative
14 Plaintiff's PHI/PII, in combination with Representative Plaintiff's name, being placed in the
15 hands of unauthorized third parties/criminals.

16 24. Representative Plaintiff has a continuing interest in ensuring that Representative
17 Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendants'
18 possession, is protected and safeguarded from future breaches.

19
20 **DEFENDANTS**

21 25. Defendants are each California corporations with their principal place of business
22 at 1996 Eastman Avenue, Suite 101 Ventura, California 93003.

23 26. Defendants provide in-home nursing and hospice services.

24 27. Representative Plaintiff is informed and believes and, based thereon, alleges that,
25 at all times herein relevant, Defendants (including the Doe defendants) did business within the
26 State of California providing healthcare.

1 33. Also, in the alternative, Representative Plaintiff requests additional Subclasses as
2 necessary based on the types of PHI/PII that were compromised.

3 34. Representative Plaintiff reserves the right to amend the above definition or to
4 propose subclasses in subsequent pleadings and motions for class certification.

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

8 a. Numerosity: A class action is the only available method for the fair and
9 efficient adjudication of this controversy. The members of the Plaintiff
10 Class are so numerous that joinder of all members is impractical, if not
11 impossible. Representative Plaintiff is informed and believes and, on that
12 basis, alleges that the total number of Class Members is in the thousands of
13 individuals. Membership in the Class will be determined by analysis of
14 Defendants' records.

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

- 20 1) Whether Defendants engaged in the wrongful conduct alleged
21 herein;
- 22 2) Whether Defendants had a legal duty to Representative Plaintiff
23 and Class Members to exercise due care in collecting, storing,
24 using, and/or safeguarding their PHI/PII;
- 25 3) Whether Defendants knew or should have known of the
26 susceptibility of Defendants' data security systems to a data
27 breach;
- 28 4) Whether Defendants' security procedures and practices to
protect their systems were reasonable in light of the measures
recommended by data security experts;
- 5) Whether Defendants' failure to implement adequate data
security measures, including the sharing of Representative
Plaintiff's and Class Members' PHI/PII, allowed the Data
Breach to occur and/or worsened its effects;
- 6) Whether Defendants failed to comply with their own policies
and applicable laws, regulations, and industry standards
relating to data security;
- 7) Whether Defendants adequately, promptly, and accurately
informed Representative Plaintiff and Class Members that their
PHI/PII had been compromised;

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

- 8) How and when Defendants actually learned of the Data Breach;
- 9) Whether Defendants 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 Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of these systems, resulting in the loss of the PHI/PII of Representative Plaintiff and Class Members;
- 11) Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- 12) Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach and/or damages flowing therefrom;
- 13) Whether Defendants' actions alleged herein constitute gross negligence and whether the negligence/recklessness of any one or more individual(s) can be imputed to Defendants;
- 14) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI/PII of Representative Plaintiff and Class Members;
- 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 Defendants' 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 Defendants' wrongful conduct;
- 17) Whether Defendants continue to breach duties to Representative Plaintiff and Class Members.

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 Defendants' 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 who had sensitive PII compromised in the same way by the same conduct of Defendants. Representative Plaintiff and all Class Members face the identical threats resulting from the breach of PII without the protection of

1 encryption and adequate monitoring of user behavior and activity
2 necessary to identify those threats.

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

14 Superiority of Class Action: The damages suffered by individual
15 Class Members are significant, but may be small relative to the
16 enormous expense of individual litigation by each member. This
17 makes or may make it impractical for members of the Plaintiff Class
18 to seek redress individually for the wrongful conduct alleged herein.
19 Even if Class Members could afford such individual litigation, the
20 court system could not. Should separate actions be brought or be
21 required to be brought, by each individual member of the Plaintiff
22 Class, the resulting multiplicity of lawsuits would cause undue
23 hardship and expense for the Court and the litigants. The
24 prosecution of separate actions would also create a risk of
25 inconsistent rulings which might be dispositive of the interests of
26 other Class Members who are not parties to the adjudications and/or
27 may substantially impede their ability to adequately protect their
28 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.

36. 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.

37. This class action is also appropriate for certification because Defendants have acted
and/or have refused to act on grounds generally applicable to the Class(es), thereby requiring the
Court's imposition of uniform relief to ensure compatible standards of conduct toward Class
Members and making final injunctive relief appropriate with respect to the Class(es) in their
entireties. Defendants' policies/practices challenged herein apply to and affect Class Members
uniformly and Representative Plaintiff's challenge of these policies/practices and conduct hinges

1 on Defendants’ conduct with respect to the Class in its entirety, not on facts or law applicable only
2 to the Representative Plaintiff.

3 38. Unless a Class-wide injunction is issued, Defendants’ violations may continue, and
4 Defendants may continue to act unlawfully as set forth in this Complaint.

5
6
7 **COMMON FACTUAL ALLEGATIONS**

8 **The Cyberattack**

9 39. In the course of the Data Breach, one or more unauthorized third parties accessed
10 Class Members’ sensitive data including, but not limited to, HIC Numbers, dates of birth, medical
11 conditions, medical reference numbers, demographic information, private health insurance
12 providers, and private health plan numbers. Representative Plaintiff was among the individuals
13 whose data was accessed in the Data Breach.

14 40. Representative Plaintiff was provided the information detailed above upon her
15 receipt of a letter from Defendant, dated January 20, 2023. Representative Plaintiff was not aware
16 of the Data Breach—or even that Defendants were still in possession of her data until receiving
17 that letter. After receiving the letter, Plaintiff was particularly anxious regarding the release of her
18 data as Defendant had taken photographs of her in the course of her treatment.

19
20 **Defendants’ Failed Response to the Breach**

21 41. Upon information and belief, the unauthorized third-party cybercriminals gained
22 access to Representative Plaintiff’s and Class Members’ PHI/PII with the intent of engaging in
23 misuse of the PHI/PII, including marketing and selling Representative Plaintiff’s and Class
24 Members’ PII. Since the Data Breach, Plaintiff has received spam emails targeted towards her
25 medical condition.

26 42. Not until nearly an entire year after they claim to have discovered the Data Breach
27 did Defendants begin sending the Notice to persons whose PHI/PII Defendants confirmed was
28

1 | potentially compromised as a result of the Data Breach. The Notice provided basic details of the
2 | Data Breach and Defendant’s recommended next steps.

3 | 43. The Notice included, *inter alia*, allegations that Defendants had learned of the Data
4 | Breach on February 19, 2022 and had taken steps to respond.

5 | 44. Defendants had and continue to have obligations created by HIPAA, applicable
6 | federal and state law as set forth herein, reasonable industry standards, common law, and their own
7 | assurances and representations to keep Representative Plaintiff’s and Class Members’ PHI/PII
8 | confidential and to protect such PHI/PII from unauthorized access.

9 | 45. Representative Plaintiff and Class Members were required to provide their PHI/PII
10 | to Defendants in order to receive healthcare, and as part of providing healthcare, Defendants
11 | created, collected, and stored Representative Plaintiff and Class Members with the reasonable
12 | expectation and mutual understanding that Defendants would comply with their obligations to
13 | keep such information confidential and secure from unauthorized access.

14 | 46. Despite this, Representative Plaintiff and the Class Members remain, even today,
15 | in the dark regarding what particular data was stolen, the particular malware used, and what steps
16 | are being taken, if any, to secure their PHI/PII going forward. Representative Plaintiff and Class
17 | Members are, thus, left to speculate as to where their PHI/PII ended up, who has used it and for
18 | what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact
19 | of the Data Breach and how exactly Defendants intend to enhance their information security
20 | systems and monitoring capabilities so as to prevent further breaches.

21 | 47. Representative Plaintiff’s and Class Members’ PHI/PII may end up for sale on the
22 | dark web, or simply fall into the hands of companies that will use the detailed PHI/PII for targeted
23 | marketing without the approval of Representative Plaintiff and/or Class Members. Either way,
24 | unauthorized individuals can now easily access the PHI/PII of Representative Plaintiff and Class
25 | Members.

26 |
27 |
28 |

1 **Defendants Collected/Stored Class Members' PHI/PII**

2 48. Defendants acquired, collected, stored and assured reasonable security over
3 Representative Plaintiff's and Class Members' PHI/PII.

4 49. As a condition of their relationships with Representative Plaintiff and Class
5 Members, Defendants required that Representative Plaintiff and Class Members entrust
6 Defendants with highly sensitive and confidential PHI/PII. Defendants, in turn, stored that
7 information on Defendants' system that was ultimately affected by the Data Breach.

8 50. By obtaining, collecting, and storing Representative Plaintiff's and Class Members'
9 PHI/PII, Defendants assumed legal and equitable duties and knew or should have known that they
10 were thereafter responsible for protecting Representative Plaintiff's and Class Members' PHI/PII
11 from unauthorized disclosure.

12 51. Representative Plaintiff and Class Members have taken reasonable steps to
13 maintain the confidentiality of their PHI/PII. Representative Plaintiff and Class Members relied
14 on Defendants to keep their PHI/PII confidential and securely maintained, to use this information
15 for business and healthcare purposes only, and to make only authorized disclosures of this
16 information.

17 52. Defendants could have prevented the Data Breach, which began no later than
18 February 19, 2022, by properly securing and encrypting and/or more securely encrypting their
19 servers generally, as well as Representative Plaintiff's and Class Members' PHI/PII.

20 53. Defendants' negligence in safeguarding Representative Plaintiff's and Class
21 Members' PHI/PII is exacerbated by repeated warnings and alerts directed to protecting and
22 securing sensitive data, as evidenced by the trending data breach attacks in recent years.

23 54. The healthcare industry has experienced a large number of high-profile
24 cyberattacks even in just the short period preceding the filing of this Complaint and cyberattacks,
25 generally, have become increasingly more common. More healthcare data breaches were reported
26
27
28

1 in 2020 than in any other year, showing a 25% increase.³ Additionally, according to the HIPAA
2 Journal, the largest healthcare data breaches have been reported in April 2021.⁴

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

10 56. Due to the high-profile nature of these breaches, and other breaches of its kind,
11 Defendants were and/or certainly should have been on notice and aware of such attacks occurring
12 in the healthcare industry and, therefore, should have assumed and adequately performed the duty
13 of preparing for such an imminent attack. This is especially true given that Defendants are large,
14 sophisticated operations with the resources to put adequate data security protocols in place.

15 57. Yet, despite the prevalence of public announcements of data breach and data
16 security compromises, Defendants failed to take appropriate steps to protect Representative
17 Plaintiff's and Class Members' PHI/PII from being compromised.

18
19 **Defendants Had an Obligation to Protect the Stolen Information**

20 58. Defendants' failure to adequately secure Representative Plaintiff's and Class
21 Members' sensitive data breaches duties it owes Representative Plaintiff and Class Members under
22 statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to

23
24 ³ <https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/> (last accessed
November 5, 2021).

25 ⁴ <https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/> (last accessed
November 5, 2021).

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

27 ⁶ <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 ⁷ <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 keep patients' Protected Health Information private. As a covered entity, Defendants had a
2 statutory duty under HIPAA and other federal and state statutes to safeguard Representative
3 Plaintiff's and Class Members' data. Moreover, Representative Plaintiff and Class Members
4 surrendered their highly sensitive personal data to Defendants under the implied condition that
5 Defendants would keep it private and secure. Accordingly, Defendants also had an implied duty
6 to safeguard their data, independent of any statute.

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

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

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

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

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

23 64. HIPAA's Security Rule requires Defendants to do the following:

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

d. Ensure compliance by their workforce.

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

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

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

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

1 69. Defendants owed a duty to Representative Plaintiff and Class Members to design,
2 maintain and test their computer systems, servers and networks to ensure that the PHI/PII in their
3 possession was adequately secured and protected.

4 70. Defendants owed a duty to Representative Plaintiff and Class Members to create
5 and implement reasonable data security practices and procedures to protect the PHI/PII in their
6 possession, including not sharing information with other entities who maintained sub-standard data
7 security systems.

8 71. Defendants owed a duty to Representative Plaintiff and Class Members to
9 implement processes that would immediately detect a breach on their data security systems in a
10 timely manner.

11 72. Defendants owed a duty to Representative Plaintiff and Class Members to act upon
12 data security warnings and alerts in a timely fashion.

13 73. Defendants owed a duty to Representative Plaintiff and Class Members to disclose
14 if their computer systems and data security practices were inadequate to safeguard individuals'
15 PHI/PII from theft because such an inadequacy would be a material fact in the decision to entrust
16 this PHI/PII to Defendants.

17 74. Defendants owed a duty of care to Representative Plaintiff and Class Members
18 because they were foreseeable and probable victims of any inadequate data security practices.

19 75. Defendants owed a duty to Representative Plaintiff and Class Members to encrypt
20 and/or more reliably encrypt Representative Plaintiff's and Class Members' PHI/PII and monitor
21 user behavior and activity in order to identify possible threats.

22
23 **Value of the Relevant Sensitive Information**

24 76. While the greater efficiency of electronic health records translates to cost savings
25 for providers, it also comes with the risk of privacy breaches. These electronic health records
26 contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's,
27 treatment plans) that is valuable to cyber criminals. One patient's complete record can be sold for
28 hundreds of dollars on the dark web. As such, PHI/PII are valuable commodities for which a "cyber

1 black market” exists in which criminals openly post stolen payment card numbers, Social Security
2 numbers, and other personal information on a number of underground internet websites.
3 Unsurprisingly, the healthcare industry is at high risk for and acutely affected by cyberattacks.

4 77. The high value of PHI/PII to criminals is further evidenced by the prices they will
5 pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.
6 For example, personal information can be sold at a price ranging from \$40 to \$200, and bank
7 details have a price range of \$50 to \$200.⁸ Experian reports that a stolen credit or debit card number
8 can sell for \$5 to \$110 on the dark web.⁹ Criminals can also purchase access to entire company
9 data breaches from \$999 to \$4,995.¹⁰

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

15 79. These criminal activities have and will result in devastating financial and personal
16 losses to Representative Plaintiff and Class Members. For example, it is believed that certain
17 PHI/PII compromised in the 2017 Experian data breach was being used, three years later, by
18 identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will
19
20

21 ⁸ *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 ⁹ *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 ¹⁰ *In the Dark*, VPNOverview, 2019, available at:
<https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed January 21,
26 2022).

27 ¹¹ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133> (last
28 accessed January 21, 2022).

¹² <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed
January 21, 2022).

¹³ <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches> (last accessed January 21, 2022).

1 be an omnipresent threat for Representative Plaintiff and Class Members for the rest of their lives.
2 They will need to remain constantly vigilant.

3 80. The FTC defines identity theft as “a fraud committed or attempted using the
4 identifying information of another person without authority.” The FTC describes “identifying
5 information” as “any name or number that may be used, alone or in conjunction with any other
6 information, to identify a specific person,” including, among other things, “[n]ame, Social Security
7 number, date of birth, official State or government issued driver’s license or identification number,
8 alien registration number, government passport number, employer or taxpayer identification
9 number.”

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

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

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

25
26
27
28

1 [L]aw enforcement officials told us that in some cases, stolen data may be held for
2 up to a year or more before being used to commit identity theft. Further, once stolen
3 data have been sold or posted on the Web, fraudulent use of that information may
4 continue for years. As a result, studies that attempt to measure the harm resulting
5 from data breaches cannot necessarily rule out all future harm.¹⁴

6 84. The harm to Representative Plaintiff and Class Members is especially acute given
7 the nature of the leaked data. Medical identity theft is one of the most common, most expensive,
8 and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, “medical-
9 related identity theft accounted for 43 percent of all identity thefts reported in the United States in
10 2013,” which is more than identity thefts involving banking and finance, the government and the
11 military, or education.¹⁵

12 85. “Medical identity theft is a growing and dangerous crime that leaves its victims
13 with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy
14 Forum. “Victims often experience financial repercussions and worse yet, they frequently discover
15 erroneous information has been added to their personal medical files due to the thief’s activities.”¹⁶

16 86. When cyber criminals access financial information, health insurance information
17 and other personally sensitive data—as they did here—there is no limit to the amount of fraud to
18 which Defendants may have exposed Representative Plaintiff and Class Members.

19 87. A study by Experian found that the average total cost of medical identity theft is
20 “about \$20,000” per incident, and that a majority of victims of medical identity theft were forced
21 to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.¹⁷ Almost
22 half of medical identity theft victims lose its healthcare coverage as a result of the incident, while
23

24
25 ¹⁴ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
<http://www.gao.gov/new.items/d07737.pdf> (last accessed January 21, 2022).

26 ¹⁵ 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 January 21, 2022).

27 ¹⁶ *Id.*

28 ¹⁷ 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 January 21, 2022).

1 nearly one-third saw its insurance premiums rise, and forty percent were never able to resolve its
2 identity theft at all.¹⁸

3 88. And data breaches are preventable.¹⁹ As Lucy Thompson wrote in the DATA
4 BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could
5 have been prevented by proper planning and the correct design and implementation of appropriate
6 security solutions.”²⁰ She added that “[o]rganizations that collect, use, store, and share sensitive
7 personal data must accept responsibility for protecting the information and ensuring that it is not
8 compromised”²¹

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

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

24
25 ¹⁸ *Id.*; see also Healthcare Data Breach: What to Know About them and What to Do After One,
26 EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/> (last accessed January 21, 2022).

27 ¹⁹ Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in*
DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

28 ²⁰ *Id.* at 17.

²¹ *Id.* at 28.

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

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

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

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

14 93. Among these duties, Defendants were expected:

- 15 a. to exercise reasonable care in obtaining, retaining, securing, safeguarding,
16 deleting and protecting the PHI/PII in their possession;
- 17 b. to protect Representative Plaintiff's and Class Members' PHI/PII using
18 reasonable and adequate security procedures and systems that were/are
19 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.

25 94. Defendants knew, or should have known, that the PHI/PII was private and
26 confidential and should be protected as private and confidential and, thus, Defendants 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.

95. Defendants knew, or should have known, of the risks inherent in collecting and
storing PHI/PII, the vulnerabilities of their data security systems, and the importance of adequate
security. Defendants knew about numerous, well-publicized data breaches.

1 96. Defendants knew, or should have known, that their data systems and networks did
2 not adequately safeguard Representative Plaintiff's and Class Members' PHI/PII.

3 97. Only Defendants were in the position to ensure that their systems and protocols
4 were sufficient to protect the PHI/PII Representative Plaintiff and Class Members had entrusted to
5 them.

6 98. Defendants breached their duties to Representative Plaintiff and Class Members by
7 failing to provide fair, reasonable, or adequate computer systems and data security practices to
8 safeguard the PHI/PII of Representative Plaintiff and Class Members.

9 99. Because Defendants knew that a breach of their systems could damage thousands
10 of individuals, including Representative Plaintiff and Class Members, Defendants had a duty to
11 adequately protect their data systems and the PHI/PII contained thereon.

12 100. Representative Plaintiff's and Class Members' willingness to entrust Defendants
13 with their PHI/PII was predicated on the understanding that Defendants would take adequate
14 security precautions. Moreover, only Defendants had the ability to protect their systems and the
15 PHI/PII they stored on them from attack. Thus, Defendants had a special relationship with
16 Representative Plaintiff and Class Members.

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

21 102. Defendants breached their general duty of care to Representative Plaintiff and Class
22 Members in, but not necessarily limited to, the following ways:

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

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. by failing to provide adequate supervision and oversight of the PHI/PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third-party to gather PHI/PII of Representative Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent.
- e. by failing to adequately train their 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.

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

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

105. The law further imposes an affirmative duty on Defendants 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.

106. Defendants breached their duty to notify Representative Plaintiff and Class Members of the unauthorized access by waiting nearly 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, Defendants have not provided sufficient information to Representative Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach their disclosure obligations to Representative Plaintiff and Class Members.

1 107. Further, through their failure to provide timely and clear notification of the Data
2 Breach to Representative Plaintiff and Class Members, Defendants prevented Representative
3 Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI/PII.

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

10 109. Defendants’ wrongful actions, inactions, and omissions constituted (and continue
11 to constitute) common law negligence.

12 110. The damages Representative Plaintiff and Class Members have suffered (as alleged
13 above) and will suffer were and are the direct and proximate result of Defendants’ grossly
14 negligent conduct.

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

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

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

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

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

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

21
22 **SECOND CAUSE OF ACTION**
Breach of Implied Contract

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

25 117. Through their course of conduct, Defendants, Representative Plaintiff, and Class
26 Members entered into implied contracts for Defendants to implement data security adequate to
27 safeguard and protect the privacy of Representative Plaintiff's and Class Members' PHI/PII.
28

1 118. As part of this contract, Defendants required Representative Plaintiff and Class
2 Members to provide and entrust to Defendants, *inter alia*, HIC Numbers, dates of birth, medical
3 conditions, medical reference numbers, demographic information, private health insurance
4 providers, and private health plan numbers Defendants solicited and invited Representative
5 Plaintiff and Class Members to provide their PHI/PII as part of Defendants' regular business
6 practices. Representative Plaintiff and Class Members accepted Defendants' offers and provided
7 their PHI/PII thereto in exchange for medical services compliant with all state and federal
8 regulations, including HIPAA.

9 119. As patients, Plaintiff and Class Members had the reasonable expectation that all
10 relevant state and federal regulations were being followed as part of the services received.
11 Compliance with all applicable state and federal regulations would be implicit in offering services
12 as a licensed medical entity in the State of California.

13 120. As a condition of being patients/clients thereof, Representative Plaintiff and Class
14 Members provided and entrusted their PHI/PII to Defendants. In so doing, Representative Plaintiff
15 and Class Members entered into implied contracts with Defendants by which Defendants agreed
16 to safeguard and protect such non-public information, to keep such information secure and
17 confidential, and to timely and accurately notify Representative Plaintiff and Class Members if
18 their data had been breached and compromised or stolen as in compliance with all regulations.

19 121. A meeting of the minds occurred when Representative Plaintiff and Class Members
20 agreed to, and did, provide their PHI/PII to Defendants, in exchange for, amongst other things, the
21 protection of their PHI/PII and medical services received.

22 122. Representative Plaintiff and Class Members fully performed their obligations under
23 the implied contracts with Defendants including payment by themselves or submission of their
24 claims to insurance or other third-party payors.

25 123. Defendants breached the implied contracts they made with Representative Plaintiff
26 and Class Members by failing to safeguard and protect their PHI/PII in compliance with all
27 applicable regulations and by failing to provide timely and accurate notice to them that their
28 PHI/PII was compromised as a result of the Data Breach.

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


- a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
 - b. requiring Defendants 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 Defendants 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;
 - d. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;
 - e. prohibiting Defendants from maintaining Representative Plaintiff's and Class Members' PHI/PII on a cloud-based database;
 - f. requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants network is compromised, hackers cannot gain access to other portions of Defendants' systems;
 - g. requiring Defendants to conduct regular database scanning and securing checks;
 - h. requiring Defendants 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;
 - i. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting PHI/PII;
 - j. requiring Defendants to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendants' networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;
 - k. requiring Defendants 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.
- 5. For prejudgment interest on all amounts awarded, at the prevailing legal rate;
 - 6. For an award of attorneys' fees, costs and litigation expenses, as allowed by law;
 - 7. 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 15, 2023

COLE & VAN NOTE

By: 

Laura Van Note, Esq.
Attorneys for Representative Plaintiff

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
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