

1 Scott Edward Cole, Esq. (S.B. #160744)
Laura Grace Van Note, Esq. (S.B. #310160)
2 Cody Alexander Bolce, Esq. (S.B. #322725)
COLE & VAN NOTE
3 555 12th Street, Suite 1725
Oakland, California 94607
4 Telephone: (510) 891-9800
Facsimile: (510) 891-7030
5 Email: sec@colevannote.com
Email: lvn@colevannote.com
6 Email: cab@colevannote.com
Web: www.colevannote.com
7

8 Attorneys for Representative Plaintiff
and the Plaintiff Class(es)
9

10 **UNITED STATES DISTRICT COURT**
11 **NORTHERN DISTRICT OF CALIFORNIA**
12

13 CADE NORDE, individually, and on behalf
of all others similarly situated,

14 Plaintiff,

15 vs.

16 CENTER FOR AUTISM AND RELATED
DISORDERS, INC.,

17 Defendant.
18
19
20
21
22
23

Case No.

CLASS ACTION

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

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

[JURY TRIAL DEMANDED]

24
25 Representative Plaintiff alleges as follows:

26 **INTRODUCTION**

27 1. Representative Plaintiff Cade Norde (“Representative Plaintiff”) brings this class
28 action against Defendant Center for Autism and Related Disorders, Inc. (“Defendant”) for its

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

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

1 failure to properly secure and safeguard Representative Plaintiff’s and Class Members’ personally
2 identifiable information stored within Defendant’s information network, including, without
3 limitation, clinical and treatment information such medical history and diagnosis (these types of
4 information, *inter alia*, being hereafter referred to, collectively, as “personal health information”
5 or “PHI”),¹ contact information, dates of birth, and insurance details, (these latter types of
6 information, *inter alia*, being hereafter referred to, collectively, as “personally identifiable
7 information” or “PII”),² and to properly secure and safeguard Representative Plaintiff’s and Class
8 Members’ PHI and PII stored within Defendant’s information network.

9 2. With this action, Representative Plaintiff seeks to hold Defendant responsible for
10 the harms it caused and will continue to cause Representative Plaintiff and the countless other
11 similarly situated persons in the massive and preventable cyberattack announced by Defendant in
12 October 2020, by which cybercriminals infiltrated Defendant’s inadequately protected network
13 servers and accessed highly sensitive PHI/PII and financial information which was being kept
14 unprotected (the “Data Breach”).

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

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

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

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

1 4. Defendant reported the security incident in October 2020, but it is not clear when
2 the breach occurred. Thus, it is also unclear whether Defendant promptly reported the security
3 incident to Representative Plaintiff or Class Members.

4 5. Defendant acquired, collected and stored Representative Plaintiff's and Class
5 Members' PHI/PII and/or financial information in connection with their employment or receiving
6 healthcare services from Defendant. Therefore, at all relevant times, Defendant knew, or should
7 have known, that Representative Plaintiff and Class Members would use Defendant's networks to
8 store and/or share sensitive data, including highly confidential PHI/PII.

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

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

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

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

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, 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, the PHI/PII of Representative Plaintiff
9 and Class Members was compromised through disclosure to an unknown and unauthorized third
10 party—an undoubtedly nefarious third party that seeks 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 that their information is and remains safe, and they
13 are entitled to injunctive and other equitable relief.

14
15 **JURISDICTION AND VENUE**

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

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

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

27
28

1 13. Venue is proper in this Court under 28 U.S.C. § 1391 because the events that gave
2 rise to Representative Plaintiff’s claims took place within the Northern District of California, and
3 Defendant does business in this Judicial District.

4
5 **PLAINTIFF**

6 14. Representative Plaintiff is an adult individual and, at all relevant times herein, a
7 resident of the State of California. Representative Plaintiff is a victim of the Data Breach.

8 15. Defendant received highly sensitive personal information from Representative
9 Plaintiff in connection with her employment with Defendant. As a result, Representative Plaintiff’s
10 information was among the data accessed by an unauthorized third-party in the Data Breach.

11 16. At all times herein relevant, Representative Plaintiff is and was a member of each
12 of the Classes.

13 17. As required in order to obtain services from Defendant, Representative Plaintiff
14 provided Defendant with highly sensitive personal, financial, health, and insurance information.

15 18. Representative Plaintiff’s PHI/PII was exposed in the Data Breach because
16 Defendant stored and/or shared Representative Plaintiff’s PHI/PII and financial information. Her
17 PHI/PII and financial information was within the possession and control of Defendant at the time
18 of the Data Breach.

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

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

27 21. 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

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

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

1 of her privacy, as well as anxiety over the impact of cybercriminals accessing and using her
2 PHI/PII and/or financial information.

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

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

10
11 **DEFENDANT**

12 24. Defendant is a California corporation with a principal place of business located at
13 21600 Oxnard Street #1800, Woodland Hills, CA 91367.

14 25. Defendant provides healthcare, remote clinical services, training programs, and
15 specialized outpatient services.³ Defendant provides services at 221 locations in 24 states.⁴

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

21
22 **CLASS ACTION ALLEGATIONS**

23 27. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a),
24 (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of himself and the following
25 classes/subclass(es) (collectively, the “Class”):
26
27

28 ³ See <https://www.centerforautism.com/services/> .

⁴ See <https://www.centerforautism.com/locations/> .

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

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

Nationwide Class:

“All individuals within the United States of America whose PHI/PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach announced by Defendant in or around October 2020.”

California Subclass:

“All individuals within the State of California whose PII/PHI was stored by Defendant and/or was exposed to unauthorized third parties as a result of the data breach announced by Defendant in or around October 2020.”

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

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

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

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

- a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff is informed and believe and, on that basis, allege that the total number of Class Members is in the hundreds of thousands of individuals. Membership in the classes will be determined by analysis of Defendant’s records.
- b. Commonality: Representative Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

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

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

- 1) Whether Defendant had a legal duty to Representative Plaintiff and the Classes to exercise due care in collecting, storing, using and/or safeguarding their PII/PHI;
 - 2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;
 - 3) Whether Defendant’s security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;
 - 4) Whether Defendant’s failure to implement adequate data security measures allowed the Data Breach to occur;
 - 5) Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
 - 6) Whether Defendant adequately, promptly, and accurately informed Representative Plaintiff and Class Members that their PII/PHI 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 the PII/PHI of Representative Plaintiff and Class Members;
 - 9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
 - 10) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Representative Plaintiff and Class Members;
 - 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;
 - 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 Classes. Representative Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant’s common course of conduct in violation of law, as alleged herein.
- d. Adequacy of Representation: Representative Plaintiff in this class action is adequate representative of each of the Plaintiff Classes in that the Representative Plaintiff has the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in its entirety. Representative Plaintiff anticipates no management difficulties in this litigation.

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

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

13 32. This class action is also appropriate for certification because Defendant has acted
14 or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's
15 imposition of uniform relief to ensure compatible standards of conduct toward the Class Members
16 and making final injunctive relief appropriate with respect to the Class(es) in its/their entirety.
17 Defendant's policies and practices challenged herein apply to and affect Class Members uniformly
18 and Representative Plaintiff's challenge of these policies and practices hinges on Defendant's
19 conduct with respect to the Class(es) in its/their entirety, not on facts or law applicable only to
20 Representative Plaintiff.

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

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

28 **COMMON FACTUAL ALLEGATIONS**

The Cyberattack

35. In the course of the Data Breach, one or more unauthorized third-parties accessed
Class Members' sensitive data including, but not limited to, clinical and treatment information

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

1 such medical history and diagnosis, contact information, dates of birth, and insurance details.
2 Representative Plaintiff was among the individuals whose data was accessed in the Data Breach.

3 36. Defendant provided this information in a sample notice sent to the California
4 Attorney General dated October 16, 2020.⁵

5 37. Upon information and belief, the unauthorized third-party cybercriminals gained
6 access to Representative Plaintiff's and Class Members' PHI/PII and financial information with
7 the intent of engaging in misuse of the PHI/PII and financial information, including marketing and
8 selling Representative Plaintiff's and Class Members' PHI/PII.

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

14 39. Representative Plaintiff and Class Members were required to provide their PHI/PII
15 and financial information to Defendant with the reasonable expectation and mutual understanding
16 that Defendant would comply with its obligations to keep such information confidential and secure
17 from unauthorized access.

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

24 41. Representative Plaintiff's and Class Members' PHI/PII and financial information
25 may end up for sale on the dark web, or simply fall into the hands of companies that will use the
26 detailed PHI/PII and financial information for targeted marketing without the approval of
27

28 ⁵ https://oag.ca.gov/system/files/Notice%20of%20Breach%20-%20CARD%20%28patients%29_PROOF.pdf (last accessed January 28, 2022).

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

1 Representative Plaintiff and/or Class Members. Either way, unauthorized individuals can now
2 easily access the PHI/PII and/or financial information of Representative Plaintiff and Class
3 Members.

4
5 **Defendant Collected/Stored Class Members' PHI/PII and Financial Information**

6 42. Defendant acquired, collected, and stored and assured reasonable security over
7 Representative Plaintiff's and Class Members' PHI/PII and financial information.

8 43. As a condition of its relationships with Representative Plaintiff and Class Members,
9 Defendant required that Representative Plaintiff and Class Members entrust Defendant with highly
10 sensitive and confidential PHI/PII and financial information.

11 44. By obtaining, collecting, and storing Representative Plaintiff's and Class Members'
12 PHI/PII and financial information, Defendant assumed legal and equitable duties and knew or
13 should have known that they were thereafter responsible for protecting Representative Plaintiff's
14 and Class Members' PHI/PII and financial information from unauthorized disclosure.

15 45. Representative Plaintiff and Class Members have taken reasonable steps to
16 maintain the confidentiality of their PHI/PII and financial information. Representative Plaintiff
17 and Class Members relied on Defendant to keep their PHI/PII and financial information
18 confidential and securely maintained, to use this information for business and healthcare purposes
19 only, and to make only authorized disclosures of this information.

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

23 47. Defendant's negligence in safeguarding Representative Plaintiff's and Class
24 Members' PHI/PII and financial information is exacerbated by repeated warnings and alerts
25 directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks
26 in recent years.

27 48. The healthcare industry has experienced a large number of high-profile
28 cyberattacks even in just the short period preceding the filing of this Complaint and cyberattacks,

1 generally, have become increasingly more common. More healthcare data breaches were reported
 2 in 2020 than in any other year, showing a 25% increase.⁶ Additionally, according to the HIPAA
 3 Journal, the largest healthcare data breaches have been reported in April 2021.⁷

4 49. For example, Universal Health Services experienced a cyberattack on September
 5 29, 2020 that appears similar to the attack on Defendant. As a result of this attack, Universal Health
 6 Services suffered a four-week outage of its systems which caused as much as \$67 million in
 7 recovery costs and lost revenue.⁸

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

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

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

18 52. Defendant's failure to adequately secure Representative Plaintiff's and Class
 19 Members' sensitive data breaches duties it owes Representative Plaintiff and Class Members under
 20 statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to
 21 keep patients' Protected Health Information private. As a covered entity, Defendant has a statutory
 22 duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiff's and
 23 Class Members' data. Moreover, Representative Plaintiff and Class Members surrendered their
 24 highly sensitive personal data to Defendant under the implied condition that Defendant would keep
 25

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

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

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

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

1 it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data,
2 independent of any statute.

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

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

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

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

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

19
20 58. HIPAA’s Security Rule requires Defendant to do the following:
21 a. Ensure the confidentiality, integrity, and availability of all electronic protected
22 health information the covered entity or business associate creates, receives,
23 maintains, or transmits;
24 b. Protect against any reasonably anticipated threats or hazards to the security or
25 integrity of such information;
26 c. Protect against any reasonably anticipated uses or disclosures of such
27 information that are not permitted; and
28 d. Ensure compliance by its workforce.

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

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 and financial information in
19 Defendant’s possession from being compromised, lost, stolen, accessed, and misused by
20 unauthorized persons. Defendant owed a duty to Representative Plaintiff and Class Members to
21 provide reasonable security, including consistency with industry standards and requirements, and
22 to ensure that its computer systems, networks, and protocols adequately protected the PHI/PII and
23 financial information of Representative Plaintiff and Class Members.

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 the PHI/PII and
26 financial information in its 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 the PHI/PII and financial

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

1 information in its possession, including not sharing information with other entities who maintained
2 sub-standard data 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 and/or financial information from theft because such an inadequacy would be a material
11 fact in the decision to entrust this PHI/PII and/or financial information to Defendants.

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 financial
16 information and monitor 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, RX's,
22 treatment plans) that is valuable to cyber criminals. One patient's complete record can be sold for
23 hundreds of dollars on the dark web. As such, PHI/PII and financial information 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. Unsurprisingly, the healthcare industry is at high risk for and
27 acutely affected by cyberattacks.

28

1 71. The high value of PHI/PII and financial information to criminals is further
 2 evidenced by the prices they will pay through the dark web. Numerous sources cite dark web
 3 pricing for stolen identity credentials. For example, personal information can be sold at a price
 4 ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.⁹ Experian reports
 5 that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹⁰ Criminals can
 6 also purchase access to entire company data breaches from \$999 to \$4,995.¹¹

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

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

18 74. The FTC defines identity theft as “a fraud committed or attempted using the
 19 identifying information of another person without authority.” The FTC describes “identifying
 20 information” as “any name or number that may be used, alone or in conjunction with any other
 21

22 ⁹ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct.
 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed July 28, 2021).

23 ¹⁰ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.
 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed November 5, 2021).

24 ¹¹ *In the Dark*, VPNOverview, 2019, available at:
 25 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed January 21,
 26 2022).

26 ¹² <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133> (last
 27 accessed January 21, 2022).

27 ¹³ <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed
 28 January 21, 2022).

28 ¹⁴ <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches> (last accessed January 21, 2022).

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

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

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

24 [L]aw enforcement officials told us that in some cases, stolen data may be held for
 25 up to a year or more before being used to commit identity theft. Further, once stolen
 26 data have been sold or posted on the Web, fraudulent use of that information may
 27 continue for years. As a result, studies that attempt to measure the harm resulting
 from data breaches cannot necessarily rule out all future harm.¹⁵

28 ¹⁵ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
<http://www.gao.gov/new.items/d07737.pdf> (last accessed January 21, 2022).

1 78. The harm to Representative Plaintiff and Class Members is especially acute given
 2 the nature of the leaked data. Medical identity theft is one of the most common, most expensive,
 3 and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, “medical-
 4 related identity theft accounted for 43 percent of all identity thefts reported in the United States in
 5 2013,” which is more than identity thefts involving banking and finance, the government and the
 6 military, or education.¹⁶

7 79. “Medical identity theft is a growing and dangerous crime that leaves its victims
 8 with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy
 9 Forum. “Victims often experience financial repercussions and worse yet, they frequently discover
 10 erroneous information has been added to their personal medical files due to the thief’s activities.”¹⁷

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

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

20 82. And data breaches are preventable.²⁰ As Lucy Thompson wrote in the DATA
 21 BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could
 22 have been prevented by proper planning and the correct design and implementation of appropriate

23
 24 ¹⁶ 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).

25 ¹⁷ *Id.*

26 ¹⁸ 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).

27 ¹⁹ *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 January 21, 2022).

28 ²⁰ Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in*
 DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

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

1 security solutions.”²¹ She added that “[o]rganizations that collect, use, store, and share sensitive
2 personal data must accept responsibility for protecting the information and ensuring that it is not
3 compromised”²²

4 83. Most of the reported data breaches are a result of lax security and the failure to
5 create or enforce appropriate security policies, rules, and procedures . . . Appropriate information
6 security controls, including encryption, must be implemented and enforced in a rigorous and
7 disciplined manner so that a *data breach never occurs*.²³

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

17 85. Defendant disregarded the rights of Representative Plaintiff and Class Members by,
18 *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and
19 reasonable measures to ensure that its 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 and/or financial information; (iii) failing to take standard and reasonably available steps
23 to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an
24 unreasonable duration of time; and (v) failing to provide Representative Plaintiff and Class
25 Members prompt and accurate notice of the Data Breach.

26
27
28 ²¹ *Id.* at 17.

²² *Id.* at 28.

²³ *Id.*

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of the Nationwide Class)

1
2
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 financial information and to use commercially reasonable methods to do so. Defendant took
8 on this obligation upon accepting and storing the PHI/PII and financial information of
9 Representative Plaintiff and Class Members in its computer systems and on its networks.

10 88. Among these duties, Defendant were expected:

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

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

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

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 and financial
information.

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

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

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

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 and financial information contained thereon.

10 95. Representative Plaintiff's and Class Members' willingness to entrust Defendant
11 with their PHI/PII and financial information was predicated on the understanding that Defendant
12 would take adequate security precautions. Moreover, only Defendant had the ability to protect its
13 systems and the PHI/PII and financial information they stored on them from attack. Thus,
14 Defendant had a special relationship with Representative 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 financial information and promptly notify them about the Data Breach. These "independent duties"
18 are untethered to any contract between Defendant and Representative Plaintiff and/or the
19 remaining Class Members.

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

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

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

- 1 d. by failing to provide adequate supervision and oversight of the PHI/PII and
2 financial information with which they were and are entrusted, in spite of the
3 known risk and foreseeable likelihood of breach and misuse, which
4 permitted an unknown third party to gather PHI/PII and financial
5 information of Representative Plaintiff and Class Members, misuse the
6 PHI/PII and intentionally disclose it to others without consent.
- 7 e. by failing to adequately train its employees to not store PHI/PII and
8 financial information longer than absolutely necessary;
- 9 f. by failing to consistently enforce security policies aimed at protecting
10 Representative Plaintiff's and the Class Members' PHI/PII and financial
11 information;
- 12 g. by failing to implement processes to quickly detect data breaches, security
13 incidents, or intrusions; and
- 14 h. by failing to encrypt Representative Plaintiff's and Class Members' PHI/PII
15 and financial information and monitor user behavior and activity in order to
16 identify possible threats.

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

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

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

27 101. Defendant breached its duty to notify Representative Plaintiff and Class Members
28 of the unauthorized access by waiting months 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.

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

1 102. Further, through its failure to provide timely and clear notification of the Data
2 Breach to Representative Plaintiff and Class Members, Defendant prevented Representative
3 Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI/PII and
4 financial information, and to access their medical records and histories.

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

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

14 105. The damages Representative Plaintiff and Class Members have suffered (as alleged
15 above) and will suffer were and are the direct and proximate result of Defendant’s grossly
16 negligent conduct.

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

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

28

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

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

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

24 111. Additionally, as a direct and proximate result of Defendant's negligence and
25 negligence *per se*, Representative Plaintiff and Class Members have suffered and will suffer the
26 continued risks of exposure of their PHI/PII and financial information, which remain in
27 Defendant's possession and are subject to further unauthorized disclosures so long as Defendant
28

1 fails to undertake appropriate and adequate measures to protect the PHI/PII and financial
2 information in its continued possession.

3
4 **SECOND CLAIM FOR RELIEF**
5 **Confidentiality of Medical Information Act**
6 **(Cal. Civ. Code §56, *et seq.*)**
7 **(On behalf of the California Subclass)**

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

10 113. Under California Civil Code §56.06, Defendant is deemed a “provider of health
11 care, health care service plan, or contractor” and is, therefore, subject to the CMIA, California
12 Civil Code §§ 56.10(a), (d) (e), 56.36(b), 56.101(a) and (b).

13 114. Under the CMIA, California Civil Code §56.05(k), California Subclass Members
14 (except employees of Defendant whose records may have been accessed) are deemed “patients.”

15 115. As defined in the CMIA, California Civil Code §56.05(j), Defendant disclosed
16 “medical information” to unauthorized persons without obtaining consent, in violation of
17 §56.10(a). Defendant’s misconduct, including failure to adequately detect, protect, and prevent
18 unauthorized disclosure, directly resulted in the unauthorized disclosure of Representative
19 Plaintiff’s and California Subclass Members’ PHI/PII and financial information to unauthorized
20 persons.

21 116. Defendant’s misconduct, including protecting and preserving the confidential
22 integrity of its clients’/customers’/employees’ PHI/PII and financial information, resulted in
23 unauthorized disclosure of sensitive and confidential PII that belongs to Representative Plaintiff
24 and California Subclass Members to unauthorized persons, breaching the confidentiality of that
25 information, thereby violating California Civil Code §§ 56.06 and 56.101(a).

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

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

1 118. Representative Plaintiff and California Subclass Members were injured and have
2 suffered damages, as described above, from Defendant's illegal disclosure and negligent release
3 of their PHI/PII and financial information in violation of Cal. Civ. Code §§ 56.10 and 56.101 and,
4 therefore, seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal
5 statutory damages of \$1,000, punitive damages of \$3,000, injunctive relief, and attorneys' fees and
6 costs.

7
8 **THIRD CLAIM FOR RELIEF**
9 **Invasion of Privacy**
10 **(On behalf of the Nationwide Class)**

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

13 120. Representative Plaintiff and Class Members had a legitimate expectation of privacy
14 to their PHI/PII and financial information and were entitled to the protection of this information
15 against disclosure to unauthorized third-parties.

16 121. Defendant owed a duty to Representative Plaintiff and Class Members to keep their
17 PHI/PII and financial information confidential.

18 122. Defendant failed to protect and released to unknown and unauthorized third-parties
19 the PHI/PII and financial information of Representative Plaintiff and Class Members.

20 123. Defendant allowed unauthorized and unknown third-parties access to and
21 examination of the PHI/PII and financial information of Representative Plaintiff and Class
22 Members, by way of Defendant's failure to protect the PHI/PII and financial information.

23 124. The unauthorized release to, custody of, and examination by unauthorized third-
24 parties of the PHI/PII and financial information of Representative Plaintiff and Class Members is
25 highly offensive to a reasonable person.

26 125. The unauthorized intrusion was into a place or thing which was private and is
27 entitled to be private. Representative Plaintiff and Class Members disclosed their PHI/PII and
28 financial information to Defendant as part of obtaining employment and/or services from
29 Defendants, but privately with an intention that the PHI/PII and financial information would be

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

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

1 kept confidential and would be protected from unauthorized disclosure. Representative Plaintiff
2 and Class Members were reasonable in their belief that such information would be kept private
3 and would not be disclosed without their authorization.

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

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

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

13 129. As a proximate result of the above acts and omissions of Defendants, the PHI/PII
14 and financial information of Representative Plaintiff and Class Members was disclosed to third-
15 parties without authorization, causing Representative Plaintiff and Class Members to suffer
16 damages.

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

24
25
26
27
28

FOURTH CLAIM FOR RELIEF
Breach of Confidence
(On behalf of the Nationwide Class)

1
2
3 131. 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.

5 132. At all times during Representative Plaintiff's and Class Members' interactions with
6 Defendants, Defendant were fully aware of the confidential nature of the PHI/PII and financial
7 information that Representative Plaintiff and Class Members provided to them.

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

13 134. Representative Plaintiff and Class Members provided their respective PHI/PII and
14 financial information to Defendant with the explicit and implicit understandings that Defendant
15 would protect and not permit the PHI/PII and financial information to be accessed by, acquired by,
16 appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or
17 viewed by unauthorized third-parties.

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

23 136. Defendant voluntarily received, in confidence, Representative Plaintiff's and Class
24 Members' PHI/PII and financial information with the understanding that the PHI/PII and financial
25 information would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by,
26 exfiltrated by, released to, stolen by, used by and/or viewed by the public or any unauthorized
27 third-parties.

28

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

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

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

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

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

17 140. The injury and harm Representative Plaintiff and Class Members suffered and will
18 continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of
19 Representative Plaintiff's and Class Members' PHI/PII and financial information. Defendant knew
20 its data systems and protocols for accepting and securing Representative Plaintiff's and Class
21 Members' PHI/PII and financial information had security and other vulnerabilities that placed
22 Representative Plaintiff's and Class Members' PHI/PII and financial information in jeopardy.

23 141. As a direct and proximate result of Defendant's breaches of confidence,
24 Representative Plaintiff and Class Members have suffered and will suffer injury, as alleged herein,
25 including, but not limited to, (a) actual identity theft; (b) the compromise, publication, and/or theft
26 of their PHI/PII and financial information; (c) out-of-pocket expenses associated with the
27 prevention, detection, and recovery from identity theft and/or unauthorized use of their PHI/PII
28 and financial information; (d) lost opportunity costs associated with effort expended and the loss

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

1 of productivity addressing and attempting to mitigate the actual and future consequences of the
2 Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest,
3 and recover from identity theft; (e) the continued risk to their PHI/PII and financial information,
4 which remains in Defendant’s possession and is subject to further unauthorized disclosures so long
5 as Defendant fails to undertake appropriate and adequate measures to protect Class Members’
6 PHI/PII and financial information in its continued possession; (f) future costs in terms of time,
7 effort, and money that will be expended as result of the Data Breach for the remainder of the lives
8 of Representative Plaintiff and Class Members; (g) the diminished value of Representative
9 Plaintiff’s and Class Members’ PHI/PII and financial information; and (h) the diminished value of
10 Defendant’s services for which Representative Plaintiff and Class Members paid and received.

11
12
13 **FIFTH CLAIM FOR RELIEF**
14 **Breach of Implied Contract**
15 **(On behalf of the Nationwide Class)**

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

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

22 144. Defendant required Representative Plaintiff and Class Members to provide and
23 entrust their PHI/PII and financial information as a condition of obtaining employment and/or
24 services from Defendant.

25 145. Defendant solicited and invited Representative Plaintiff and Class Members to
26 provide their PHI/PII and financial information as part of Defendant’s regular business practices.
27 Representative Plaintiff and Class Members accepted Defendant’s offers and provided their
28 PHI/PII and financial information to Defendants.

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

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

8 147. A meeting of the minds occurred when Representative Plaintiff and Class Members
9 agreed to, and did, provide their PHI/PII and financial information to Defendants, in exchange for,
10 amongst other things, the protection of their PHI/PII and financial information.

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

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

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

24
25 **SIXTH CLAIM FOR RELIEF**
26 **Breach of the Implied Covenant of Good Faith and Fair Dealing**
(On behalf of the Nationwide Class)

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

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

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

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

6 154. Defendant breached the implied covenant of good faith and fair dealing by failing
7 to maintain adequate computer systems and data security practices to safeguard PHI/PII and
8 financial information, failing to timely and accurately disclose the Data Breach to Representative
9 Plaintiff and Class Members and the continued acceptance of PHI/PII and financial information
10 and storage of other personal information after Defendant knew, or should have known, of the
11 security vulnerabilities of the systems that were exploited in the Data Breach.

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

15 **SEVENTH CLAIM FOR RELIEF**
16 **Unfair Business Practices**
17 **(Cal. Bus. & Prof. Code, §17200, et seq.)**
18 **(On behalf of the California Subclass)**

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

21 157. Representative Plaintiff and California Subclass Members further bring this cause
22 of action, seeking equitable and statutory relief to stop the misconduct of Defendant, as complained
23 of herein.

24 158. Defendant has engaged in unfair competition within the meaning of California
25 Business & Professions Code §§17200, et seq., because Defendant’s conduct is unlawful, unfair
26 and/or fraudulent, as herein alleged.

27 159. Representative Plaintiff, the California Subclass Members, and Defendant are each
28 a “person” or “persons” within the meaning of § 17201 of the California Unfair Competition Law
 (“UCL”).

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

1 160. The knowing conduct of Defendant, as alleged herein, constitutes an unlawful
2 and/or fraudulent business practice, as set forth in California Business & Professions Code
3 §§17200-17208. Specifically, Defendant conducted business activities while failing to comply
4 with the legal mandates cited herein, including HIPAA. Such violations include, but are not
5 necessarily limited to:

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

16 161. Defendant knew or should have known that its computer systems and data security
17 practices were inadequate to safeguard the PHI/PII and financial information of Representative
18 Plaintiff and California Subclass Members, deter hackers, and detect a breach within a reasonable
19 time and that the risk of a data breach was highly likely.

20 162. In engaging in these unlawful business practices, Defendant has enjoyed an
21 advantage over its competition and a resultant disadvantage to the public and California Subclass
22 Members.

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

27 164. Defendant has clearly established a policy of accepting a certain amount of
28 collateral damage, as represented by the damages to Representative Plaintiff and California

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

1 Subclass Members herein alleged, as incidental to its business operations, rather than accept the
2 alternative costs of full compliance with fair, lawful and honest business practices ordinarily borne
3 by responsible competitors of Defendant and as set forth in legislation and the judicial record.

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

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

15
16 **EIGHTH CLAIM FOR RELIEF**
17 **Unjust Enrichment**
(On behalf of the Nationwide Class)

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

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

22 169. Defendants, prior to and at the time Representative Plaintiff and Class Members
23 entrusted their PHI/PII and financial information to Defendant for the purpose of obtaining health
24 services, caused Representative Plaintiff and Class Members to reasonably believe that Defendant
25 would keep such PHI/PII and financial information secure.

26 170. Defendant was aware, or should have been aware, that reasonable patients,
27 consumers, and employees would have wanted their PHI/PII and financial information kept secure
28

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

1 and would not have contracted with Defendant, directly or indirectly, had they known that
2 Defendant's information systems were sub-standard for that purpose.

3 171. Defendant was also aware that, if the substandard condition of and vulnerabilities
4 in its information systems were disclosed, it would negatively affect Representative Plaintiff's and
5 Class Members' decisions to seek services or employment therefrom.

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

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

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

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

25
26
27
28

RELIEF SOUGHT

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

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

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

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

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

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

- a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
- c. requiring Defendant to delete and purge the PII/PHI of Representative Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiff and Class Members;
- 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’ PII/PHI;

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

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

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

- 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’ PII/PHI on a cloud-based database;
- g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant’s network is compromised, hackers cannot gain access to other portions of Defendant’s systems;
- h. requiring Defendant to conduct regular database scanning and securing checks;
- i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees’ respective responsibilities with handling PII/PHI, as well as protecting the PII/PHI of Representative 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.

- 6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;
- 7. For an award of attorneys’ fees, costs, and litigation expenses, as allowed by law;
- 8. For all other Orders, findings, and determinations identified and sought in this

Complaint.

JURY DEMAND

Representative Plaintiff, individually and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demands a trial by jury for all issues triable by jury.

Dated: January 31, 2022

COLE & VAN NOTE

By: /s/ Scott Edward Cole
Scott Edward Cole, Esq.
Attorneys for Representative Plaintiff
and the Plaintiff Class(es)

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

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