

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 12<sup>th</sup> 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 CHARLENE KENNEDY, individually, and  
on behalf of all others similarly situated,  
14

15 Plaintiff,

16 vs.

LINCARE HOLDINGS INC.,  
17

18 Defendant.  
19  
20  
21  
22

**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 IMPLIED CONTRACT;
- 5. UNFAIR BUSINESS PRACTICES;
- 6. UNJUST ENRICHMENT

**[JURY TRIAL DEMANDED]**

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

1 Representative Plaintiff alleges as follows:  
2

3 **INTRODUCTION**

4 1. Representative Plaintiff Charlene Kennedy (“Representative Plaintiff”) brings this  
5 class action against Defendant Lincare Holdings Inc. (“Defendant”) for its failure to properly  
6 secure and safeguard Representative Plaintiff’s and Class Members’ personally identifiable  
7 information stored within Defendant’s information network, including, without limitation, medical  
8 information such as, information regarding medical treatments, provider names, dates of service,  
9 diagnosis/procedure information, (these types of information, *inter alia*, being hereafter referred  
10 to, collectively, as “personal health information” or “PHI”),<sup>1</sup> account and/or record numbers,  
11 names, and dates of birth (these latter types of information, *inter alia*, being hereafter referred to,  
12 collectively, as “personally identifiable information” or “PII”).<sup>2</sup>

13 2. With this action, Representative Plaintiff seeks to hold Defendant responsible for  
14 the harms it caused and will continue to cause Representative Plaintiff and the countless other  
15 similarly situated persons in the massive and preventable cyberattack beginning as early as  
16 September 10, 2021 and discovered by Defendant on September 26, 2021, by which  
17 cybercriminals infiltrated Defendant’s inadequately protected network servers and accessed highly  
18 sensitive PHI/PII and financial information which was being kept unprotected (the “Data Breach”).

19 3. Representative Plaintiff further seeks to hold Defendant responsible for not  
20 ensuring that the PHI/PII was maintained in a manner consistent with industry, the Health  
21 Insurance Portability and Accountability Act of 1996 (“HIPPA”) Privacy Rule (45 CFR, Parts 160  
22

23 <sup>1</sup> 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 <sup>2</sup> 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).

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

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

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

3 4. While Defendant claims to have discovered the breach as early as September 26,  
4 2021, Defendant did not begin informing victims of the Data Breach until June 2022. Indeed,  
5 Representative Plaintiff and Class Members were wholly unaware of the Data Breach until  
6 she/they received letter(s) from Defendant informing them of it. In particular, the letter  
7 Representative Plaintiff received was dated June 6, 2022.

8 5. Defendant acquired, collected and stored Representative Plaintiff's and Class  
9 Members' PHI/PII and/or financial information to facilitate clinical peer review of healthcare  
10 services Representative Plaintiff and Class Members requested or received. Therefore, at all  
11 relevant times, Defendant knew, or should have known, that Representative Plaintiff and Class  
12 Members would use Defendant's networks to store and/or share sensitive data, including highly  
13 confidential PHI/PII.

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

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

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

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

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

### 18 JURISDICTION AND VENUE

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

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

1 12. Defendant routinely conducts business in California, has sufficient minimum  
2 contacts in California and has intentionally availed itself of this jurisdiction by marketing and  
3 selling products and services, and by accepting and processing payments for those products and  
4 services within California.

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

8  
9 **PLAINTIFF**

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

12 15. Defendant received highly sensitive personal, medical, and financial information  
13 from Representative Plaintiff in connection with her purchase of oxygen and/or other medical  
14 products from Defendant.

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

17 17. At all times herein relevant, Representative Plaintiff is and was a member of each  
18 of the Classes.

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

21 19. Representative Plaintiff’s PHI/PII was exposed in the Data Breach because  
22 Defendant stored and/or shared Representative Plaintiff’s PHI/PII and financial information. Her  
23 PHI/PII and financial information was within the possession and control of Defendant at the time  
24 of the Data Breach.

25 20. Representative Plaintiff received a letter from Defendant, dated June 6, 2022,  
26 informing her that her PHI/PII and/or financial information was involved in the Data Breach (the  
27 “Notice”).  
28

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



1 respiratory care is delivered in the home.”<sup>3</sup> Defendant’s operation includes dozens of subsidiaries  
2 and partners across North America.<sup>4</sup>

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

### 8 9 CLASS ACTION ALLEGATIONS

10 29. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a),  
11 (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of herself and the following  
12 classes/subclass(es) (collectively, the “Class”):

#### 13 Nationwide Class:

14 “All individuals within the United States of America whose PHI/PII and/or  
15 financial information was exposed to unauthorized third-parties as a result  
16 of the data breach occurring between September 10, 2021 and September  
17 29, 2021.”

#### 18 California Subclass:

19 “All individuals within the State of California whose PII/PHI was stored by  
20 Defendant and/or was exposed to unauthorized third parties as a result of  
21 the data breach occurring between September 10, 2021 and September 29,  
22 2021.”

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

<sup>3</sup> See <https://www.lincare.com/en/> (last accessed July 5, 2022).

<sup>4</sup> See <https://www.sec.gov/Archives/edgar/data/882235/000119312512074448/d258295dex211.htm> (last accessed July 6, 2022).

COLE & VAN NOTE  
ATTORNEYS AT LAW  
555 12<sup>TH</sup> STREET, SUITE 1725  
OAKLAND, CA 94607  
TEL: (510) 891-9600

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

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

5 33. This action has been brought and may properly be maintained as a class action  
6 under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of  
7 interest in the litigation and membership in the proposed classes 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 Classes are so numerous that joinder of all members is impractical, if not  
11 impossible. Representative Plaintiff is informed and believe and, on that  
12 basis, allege that the total number of Class Members is in the hundreds of  
13 thousands of individuals. Membership in the classes will be determined by  
14 analysis of Defendant's records.

15 b. Commonality: Representative Plaintiff and the 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 Defendant had a legal duty to Representative Plaintiff and  
21 the Classes to exercise due care in collecting, storing, using, and/or  
22 safeguarding their PII/PHI;

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

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

28 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;



COLE & VAN NOTE  
ATTORNEYS AT LAW  
555 12<sup>TH</sup> 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

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 an adequate representative of each of the Plaintiff Classes in that Representative Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in its entirety. Representative Plaintiff anticipates no management difficulties in this litigation.

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

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

1 conduct with respect to the Class(es) in its/their entirety, not on facts or law applicable only to  
2 Representative Plaintiff.

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

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

## 10 11 COMMON FACTUAL ALLEGATIONS

### 12 The Cyberattack

13 37. In the course of the Data Breach, one or more unauthorized third-parties accessed  
14 Class Members' sensitive data including, but not limited to, medical information, account or record  
15 information, names, and dates of birth. Representative Plaintiff was among the individuals whose  
16 data was accessed in the Data Breach.

17 38. Representative Plaintiff was provided the information detailed above upon her  
18 receipt of a letter from Defendant, dated June 6, 2022. She was not aware of the Data Breach until  
19 receiving that letter.

### 20 21 Defendant's Failed Response to the Breach

22 39. Not until roughly nine months after it claims to have discovered the Data Breach  
23 did Defendant begin sending the Notice to persons whose PHI/PII and/or financial information  
24 Defendant confirmed was potentially compromised as a result of the Data Breach. The Notice  
25 provided basic details of the Data Breach and Defendant' recommended next steps.

26 40. The Notice included, *inter alia*, the claims that Defendant had "identified unusual  
27 activity on certain systems within its network" on September 26, 2021, had taken steps to respond,  
28

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

1 and was continuing to investigate. It claimed that Defendant took measures to contain the attack  
2 and engaged outside cyber security experts to aid its investigation.

3 41. Upon information and belief, the unauthorized third party cybercriminals gained  
4 access to Representative Plaintiff’s and Class Members’ PHI/PII and financial information with  
5 the intent of engaging in misuse of the PHI/PII and financial information, including marketing and  
6 selling Representative Plaintiff’s and Class Members’ PHI/PII.

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

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

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

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

28

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

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

2 46. Defendant acquired, collected, and stored, and assured reasonable security over,  
3 Representative Plaintiff's and Class Members' PHI/PII and financial information.

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

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

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

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

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

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

1 in 2020 than in any other year, showing a 25% increase.<sup>5</sup> Additionally, according to the HIPAA  
 2 Journal, the largest healthcare data breaches have been reported beginning in April 2021.<sup>6</sup>

3 53. 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.<sup>7</sup> 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.<sup>8</sup> A few  
 9 months later, University of San Diego Health suffered a similar attack.<sup>9</sup>

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

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

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

20 56. Defendant's 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 <sup>5</sup> <https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/> (last accessed  
 November 5, 2021).

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

26 <sup>7</sup> <https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and> (last accessed November 5, 2021).

27 <sup>8</sup> <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 <sup>9</sup> <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, Defendant has a statutory  
 2 duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiff's and  
 3 Class Members' data. Moreover, Representative Plaintiff and Class Members surrendered their  
 4 highly sensitive personal data to Defendant under the implied condition that Defendant would keep  
 5 it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data,  
 6 independent of any statute.

7 57. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to  
 8 comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E  
 9 ("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 58. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health  
 13 Information establishes national standards for the protection of health information.

14 59. 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 60. HIPAA requires Defendant 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 61. "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 62. HIPAA's Security Rule requires Defendant 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,  
 maintains, or transmits;
- 26 b. Protect against any reasonably anticipated threats or hazards to the security or  
 27 integrity of such information;
- 28 c. Protect against any reasonably anticipated uses or disclosures of such  
 information that are not permitted; and

COLE & VAN NOTE  
ATTORNEYS AT LAW  
555 12<sup>TH</sup> 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

d. Ensure compliance by its workforce.

63. HIPAA also requires Defendant 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).

64. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant 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.”

65. Defendant was 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).

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

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

1           68. Defendant owed a duty to Representative Plaintiff and Class Members to create and  
 2 implement reasonable data security practices and procedures to protect the PHI/PII and financial  
 3 information in its possession, including not sharing information with other entities who maintained  
 4 sub-standard data security systems.

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

8           70. Defendant owed a duty to Representative Plaintiff and Class Members to act upon  
 9 data security warnings and alerts in a timely fashion.

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

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

16           73. Defendant owed a duty to Representative Plaintiff and Class Members to encrypt  
 17 and/or more reliably encrypt Representative Plaintiff's and Class Members' PHI/PII and financial  
 18 information and monitor user behavior and activity in order to identify possible threats.

19  
 20 **Value of the Relevant Sensitive Information**

21           74. While the greater efficiency of electronic health records translates to cost savings  
 22 for providers, it also comes with the risk of privacy breaches. These electronic health records  
 23 contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's,  
 24 treatment plans) that is valuable to cyber criminals. One patient's complete record can be sold for  
 25 hundreds of dollars on the dark web. As such, PHI/PII and financial information are valuable  
 26 commodities for which a "cyber black market" exists in which criminals openly post stolen  
 27 payment card numbers, Social Security numbers, and other personal information on a number of  
 28



1 underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and  
 2 acutely affected by cyberattacks.

3 75. The high value of PHI/PII and financial information to criminals is further  
 4 evidenced by the prices they will pay through the dark web. Numerous sources cite dark web  
 5 pricing for stolen identity credentials. For example, personal information can be sold at a price  
 6 ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.<sup>10</sup> Experian reports  
 7 that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.<sup>11</sup> Criminals can  
 8 also purchase access to entire company data breaches from \$999 to \$4,995.<sup>12</sup>

9 76. Between 2005 and 2019, at least 249 million people were affected by health care  
 10 data breaches.<sup>13</sup> Indeed, during 2019 alone, over 41 million healthcare records were exposed,  
 11 stolen, or unlawfully disclosed in 505 data breaches.<sup>14</sup> In short, these sorts of data breaches are  
 12 increasingly common, especially among healthcare systems, which account for 30.03% of overall  
 13 health data breaches, according to cybersecurity firm Tenable.<sup>15</sup>

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

20  
 21  
 22 <sup>10</sup> *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 <sup>11</sup> *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 <sup>12</sup> *In the Dark*, VPNOverview, 2019, available at:  
 25 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed January 21,  
 2022).

26 <sup>13</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133> (last  
 27 accessed January 21, 2022).

28 <sup>14</sup> <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed  
 January 21, 2022).

<sup>15</sup> <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches> (last accessed January 21, 2022).

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

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

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

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

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

1 continue for years. As a result, studies that attempt to measure the harm resulting  
 2 from data breaches cannot necessarily rule out all future harm.<sup>16</sup>

3  
 4 82. The harm to Representative Plaintiff and Class Members is especially acute given  
 5 the nature of the leaked data. Medical identity theft is one of the most common, most expensive,  
 6 and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, “medical-  
 7 related identity theft accounted for 43 percent of all identity thefts reported in the United States in  
 8 2013,” which is more than identity thefts involving banking and finance, the government and the  
 9 military, or education.<sup>17</sup>

10 83. “Medical identity theft is a growing and dangerous crime that leaves its victims  
 11 with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy  
 12 Forum. “Victims often experience financial repercussions and worse yet, they frequently discover  
 13 erroneous information has been added to their personal medical files due to the thief’s activities.”<sup>18</sup>

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

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

23  
 24 <sup>16</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:  
<http://www.gao.gov/new.items/d07737.pdf> (last accessed January 21, 2022).

25 <sup>17</sup> 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).

26 <sup>18</sup> *Id.*

27 <sup>19</sup> 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).

28 <sup>20</sup> *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).

1           86. And data breaches are preventable.<sup>21</sup> As Lucy Thompson wrote in the DATA  
 2 BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could  
 3 have been prevented by proper planning and the correct design and implementation of appropriate  
 4 security solutions.”<sup>22</sup> She added that “[o]rganizations that collect, use, store, and share sensitive  
 5 personal data must accept responsibility for protecting the information and ensuring that it is not  
 6 compromised . . . .”<sup>23</sup>

7           87. Most of the reported data breaches are a result of lax security and the failure to  
 8 create or enforce appropriate security policies, rules, and procedures . . . Appropriate information  
 9 security controls, including encryption, must be implemented and enforced in a rigorous and  
 10 disciplined manner so that a *data breach never occurs*.<sup>24</sup>

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

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

26 \_\_\_\_\_  
 27 <sup>21</sup> Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in*  
 DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

28 <sup>22</sup> *Id.* at 17.

<sup>23</sup> *Id.* at 28.

<sup>24</sup> *Id.*

1 to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an  
2 unreasonable duration of time; and (v) failing to provide Representative Plaintiff and Class  
3 Members prompt and accurate notice of the Data Breach.

4  
5 **FIRST CLAIM FOR RELIEF**  
6 **Negligence**  
7 **(On behalf of the Nationwide Class)**

8 90. 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 91. At all times herein relevant, Defendant owed Representative Plaintiff and Class  
11 Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII  
12 and financial information and to use commercially reasonable methods to do so. Defendant took  
13 on this obligation upon accepting and storing the PHI/PII and financial information of  
14 Representative Plaintiff and Class Members in its computer systems and on its networks.

15 92. Among these duties, Defendant were expected:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

104. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PHI/PII and financial information 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 and financial information.

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

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

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

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

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

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

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



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

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

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

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

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

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

9  
10 **SECOND CLAIM FOR RELIEF**  
11 **Confidentiality of Medical Information Act**  
12 **(Cal. Civ. Code §56, *et seq.*)**  
13 **(On behalf of the California Subclass)**

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

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

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

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

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

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

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

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

3 121. As a result of the Data Breach, unauthorized third parties viewed Representative  
4 Plaintiff's and Class Members' protected medical information.

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

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

16  
17 **THIRD CLAIM FOR RELIEF**  
18 **Invasion of Privacy**  
**(On behalf of the Nationwide Class)**

19 124. 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.

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

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

26 127. Defendant failed to protect and released to unknown and unauthorized third parties  
27 the PHI/PII and financial information of Representative Plaintiff and Class Members.  
28

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

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

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

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

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

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

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

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

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

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

6  
7 **FOURTH CLAIM FOR RELIEF**  
8 **Breach of Implied Contract**  
9 **(On behalf of the Nationwide Class)**

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

12 137. Through its course of conduct, Defendant, Representative Plaintiff, and Class  
13 Members entered into implied contracts for Defendant to implement data security adequate to  
14 safeguard and protect the privacy of Representative Plaintiff's and Class Members' PHI/PII and  
15 financial information.

16 138. Defendant required Representative Plaintiff and Class Members to provide and  
17 entrust their PHI/PII and financial information, including medical information, record or account  
18 numbers, names and dates of birth.

19 139. Defendant solicited and invited Representative Plaintiff and Class Members to  
20 provide their PHI/PII and financial information as part of Defendant's regular business practices.  
21 Representative Plaintiff and Class Members accepted Defendant's offers and provided their  
22 PHI/PII and financial information to Defendants.

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

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

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

1 141. A meeting of the minds occurred when Representative Plaintiff and Class Members  
2 agreed to, and did, provide its PHI/PII and financial information to Defendants, in exchange for,  
3 amongst other things, the protection of its PHI/PII and financial information.

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

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

10 144. As a direct and proximate result of Defendant’s above-described breach of implied  
11 contract, Representative Plaintiff and Class Members have suffered (and will continue to suffer)  
12 (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting  
13 in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting  
14 in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data;  
15 (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other  
16 economic and non-economic harm.

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

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

24 146. Representative Plaintiff and California Subclass Members further bring this cause  
25 of action, seeking equitable and statutory relief to stop the misconduct of Defendant, as complained  
26 of herein.

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

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

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

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

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

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

26           151. In engaging in these unlawful business practices, Defendant has enjoyed an  
27 advantage over its competition and a resultant disadvantage to the public and California Subclass  
28 Members.

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

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

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

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

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

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

19  
 20 **SIXTH CLAIM FOR RELIEF**  
 21 **Unjust Enrichment**  
 22 **(On behalf of the Nationwide Class)**

23 156. 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.

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

27 158. Defendants, prior to and at the time Representative Plaintiff and Class Members  
 28 entrusted their PHI/PII and financial information to Defendant for the purpose of obtaining health



1 services, caused Representative Plaintiff and Class Members to reasonably believe that Defendant  
 2 would keep such PHI/PII and financial information secure.

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

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

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

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

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

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

**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 12<sup>TH</sup> STREET, SUITE 1725  
OAKLAND, CA 94607  
TEL: (510) 891-9800

COLE & VAN NOTE  
ATTORNEYS AT LAW  
555 12<sup>TH</sup> 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 its 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: July 6, 2022

**COLE & VAN NOTE**

By: /s/ Cody A. Bolce  
Cody A. Bolce, Esq.  
Attorneys for Representative Plaintiff  
and the Plaintiff Class(es)

COLE & VAN NOTE  
ATTORNEYS AT LAW  
555 12<sup>TH</sup> 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

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Lincare Facing Class Action Lawsuit Over September 2021 Data Breach](#)

---