

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, Indiana 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 **SOUTHERN DISTRICT OF INDIANA**  
 12

13 DYLAN GILL, individually, and on  
 behalf of all others similarly situated,

14 Plaintiff,

15 vs.

16 INDIANAPOLIS NEUROSURGICAL  
 GROUP, P.C. dba GOODMAN  
 17 CAMPBELL BRAIN AND SPINE.

18 Defendant.  
 19  
 20

**Case No.**

**CLASS ACTION**

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

1. NEGLIGENCE;
2. INVASION OF PRIVACY;
3. BREACH OF IMPLIED CONTRACT;
4. UNFAIR BUSINESS PRACTICES;
5. 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 Dylan Gill (“Gill” or “Representative Plaintiff”) brings this class  
5 action against Defendant Indianapolis Neurosurgical Group, P.C. dba Goodman Campbell Brain  
6 And Spine (“Defendant”) for its failure to properly secure and safeguard Representative Plaintiff’s  
7 and Class Members’ personally identifiable information stored within Defendant’s information  
8 network, including, without limitation, medical record number, patient account number, diagnosis  
9 and treatment information, physician name, dates of service, and insurance information (this type  
10 of information, *inter alia*, being hereafter referred to, collectively, as “personal health information”  
11 or “PHI”),<sup>1</sup> names, addresses, dates of birth, Social Security numbers, email addresses, and  
12 telephone numbers (these latter types of information, *inter alia*, being hereafter referred to,  
13 collectively, as “personally identifiable information” or “PII”).<sup>2</sup>

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

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

4 4. While Defendant claims to have discovered the breach as early as May 2022,  
5 Defendant did not begin informing victims of the Data Breach until July 2022. Indeed,  
6 Representative Plaintiff and Class Members were wholly unaware of the Data Breach until  
7 she/they received letter(s) from Defendant informing them of it. In particular, the letter  
8 Representative Plaintiff received was dated July 19, 2022.

9 5. Defendant acquired, collected and stored Representative Plaintiff’s and Class  
10 Members’ PHI/PII and/or financial information in connection with its provisions of medical  
11 services Representative Plaintiff and Class Members received. Therefore, at all relevant times,  
12 Defendant knew, or should have known, that Representative Plaintiff and Class Members would  
13 use Defendant’s networks to store and/or share sensitive data, including highly confidential  
14 PHI/PII.

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

25 7. Additionally, the HIPAA Security Rule establishes national standards to protect  
26 individuals’ electronic personal health information that is created, received, used, or maintained  
27 by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and  
28

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

1 technical safeguards to ensure the confidentiality, integrity, and security of electronic protected  
2 health information.

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

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

20  
21 **JURISDICTION AND VENUE**

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

28

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

1 11. Supplemental jurisdiction to adjudicate issues pertaining to Indiana state law is  
2 proper in this Court under 28 U.S.C. §1367.

3 12. Defendant is a resident of this state and this district.

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

7  
8 **PLAINTIFF**

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

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

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

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

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

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

24 20. Representative Plaintiff received a letter from Defendant, dated July 19, 2022,  
25 informing his that his PHI/PII and/or financial information was involved in the Data Breach (the  
26 “Notice”).

27 21. As a result, Representative Plaintiff spent time dealing with the consequences of  
28 the Data Breach, which included and continues to include, time spent verifying the legitimacy and

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

1 impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-  
2 monitoring his accounts, and seeking legal counsel regarding his options for remedying and/or  
3 mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

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

7 23. Representative Plaintiff suffered lost time, annoyance, interference, and  
8 inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss  
9 of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PHI/PII  
10 and/or financial information.

11 24. Defendant’s notice states that “as a result of the incident, we do know that some of  
12 the information acquired by the attacker was made available for approximately 10 days on the dark  
13 web, which is a portion of the internet that cannot be found by search engines and is not viewable  
14 in a standard web browser and is commonly used in these types of attacks.” The knowledge that  
15 his information was available on the dark web gave him an acute sense of anxiety and  
16 embarrassment.

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

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

24  
25 **DEFENDANT**

26 27. Defendant is a Indiana corporation with a principal place of business located at  
27 13345 Illinois Street Carmel, Indiana 46032.

28

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

1 28. Defendant is a healthcare provider. It was established as the Indianapolis  
2 Neurosurgical Group in 1970 by Drs. Julius Goodman and John Russell.<sup>3</sup> It presently has programs  
3 for brain tumors, vascular issues, spine problems, trauma, neuro endovascular issues, and various  
4 interventional, functional, and pediatric treatments.<sup>4</sup>

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

10  
11 **CLASS ACTION ALLEGATIONS**

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

15 **Nationwide Class:**

16 “All individuals within the United States of America whose PHI/PII and/or  
17 financial information was exposed to unauthorized third-parties as a result  
18 of the data breach discovered on May 20, 2022.”

19 **Indiana Subclass:**

20 “All individuals within the State of Indiana whose PII/PHI was stored by  
21 Defendant and/or was exposed to unauthorized third parties as a result of  
22 the data breach discovered on May 20, 2022.”

23 31. 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> <https://www.goodmancampbell.com/about/> (last accessed August 15, 2022).

<sup>4</sup> *Id.*

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

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

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

5 34. 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 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

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.

35. 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 36. 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 37. 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 38. 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 record number, patient  
15 account number, diagnosis and treatment information, physician name, dates of service, insurance  
16 information names, addresses, dates of birth, Social Security numbers, email addresses, and  
17 telephone numbers. Representative Plaintiff was among the individuals whose data was accessed  
18 in the Data Breach.

19 39. Representative Plaintiff was provided the information detailed above upon his  
20 receipt of a letter from Defendant, dated July 19, 2022. he was not aware of the Data Breach until  
21 receiving that letter.

22  
23 **Defendant’s Failed Response to the Breach**

24 40. Not until roughly nine months after it claims to have discovered the Data Breach  
25 did Defendant begin sending the Notice to persons whose PHI/PII and/or financial information  
26 Defendant confirmed was potentially compromised as a result of the Data Breach. The Notice  
27 provided basic details of the Data Breach and Defendant’ recommended next steps.  
28

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           41. The Notice included, *inter alia*, the claims Defendant became aware that its  
2 “computer network and communications systems had been compromised through a sophisticated  
3 ransomware attack.” It further stated that it took steps to secure its system “engage a forensic  
4 analysis an incident response firm to help restore [the] affected systems, recover data, and eradicate  
5 any malicious activity from [its] system.”

6           42. The notice further stated that while Defendant wasn’t able to “verify the full nature  
7 and extent of personal information that was compromised” it knew the attackers accessed  
8 information including “medical, financial, and demographic information relating to [its] patients.”  
9 It also provided that some of this information was available on the dark web for approximately ten  
10 days.

11           43. On August 11, 2022, Defendant published an update to website in which it  
12 announced that the leak site used to share the stolen information had been reactivated by the  
13 attacker.<sup>5</sup> Accordingly, it is clear cybercriminals still possess this information.

14           44. Upon information and belief, the unauthorized third party cybercriminals gained  
15 access to Representative Plaintiff’s and Class Members’ PHI/PII and financial information with  
16 the intent of engaging in misuse of the PHI/PII and financial information, including marketing and  
17 selling Representative Plaintiff’s and Class Members’ PHI/PII.

18           45. Defendant had and continues to have obligations created by HIPAA, reasonable  
19 industry standards, common law, state statutory law, and its own assurances and representations  
20 to keep Representative Plaintiff’s and Class Members’ PHI/PII confidential and to protect such  
21 PHI/PII from unauthorized access.

22           46. Representative Plaintiff and Class Members were required to provide their PHI/PII  
23 and financial information to Defendant with the reasonable expectation and mutual understanding  
24 that Defendant would comply with its obligations to keep such information confidential and secure  
25 from unauthorized access.

26           47. Despite this, Representative Plaintiff and the Class Members remain, even today,  
27 in the dark regarding what particular data was stolen, the particular malware used, and what steps  
28

---

<sup>5</sup> <https://www.goodmancampbell.com/2022/07/important-update/> (last accessed August 15, 2022).

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

1 are being taken, if any, to secure their PHI/PII and financial information going forward.  
2 Representative Plaintiff and Class Members are left to speculate as to the full impact of the Data  
3 Breach and how exactly Defendant intends to enhance its information security systems and  
4 monitoring capabilities so as to prevent further breaches.

5 48. Representative Plaintiff’s and Class Members’ PHI/PII and financial information  
6 may end up for sale on the dark web, or simply fall into the hands of companies that will use the  
7 detailed PHI/PII and financial information for targeted marketing without the approval of  
8 Representative Plaintiff and/or Class Members. Either way, unauthorized individuals can now  
9 easily access the PHI/PII and/or financial information of Representative Plaintiff and Class  
10 Members.

11  
12 **Defendant Collected/Stored Class Members’ PHI/PII and Financial Information**

13 49. Defendant acquired, collected, and stored, and assured reasonable security over,  
14 Representative Plaintiff’s and Class Members’ PHI/PII and financial information.

15 50. As a condition of its relationships with Representative Plaintiff and Class Members,  
16 Defendant required that Representative Plaintiff and Class Members entrust Defendant with highly  
17 sensitive and confidential PHI/PII and financial information. Defendant, in turn, stored that  
18 information on its system that was ultimately affected by the Data Breach.

19 51. By obtaining, collecting, and storing Representative Plaintiff’s and Class Members’  
20 PHI/PII and financial information, Defendant assumed legal and equitable duties and knew, or  
21 should have known, that they were thereafter responsible for protecting Representative Plaintiff’s  
22 and Class Members’ PHI/PII and financial information from unauthorized disclosure.

23 52. Representative Plaintiff and Class Members have taken reasonable steps to  
24 maintain the confidentiality of their PHI/PII and financial information. Representative Plaintiff  
25 and Class Members relied on Defendant to keep their PHI/PII and financial information  
26 confidential and securely maintained, to use this information for business and healthcare purposes  
27 only, and to make only authorized disclosures of this information.  
28

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

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

4 54. Defendant's negligence in safeguarding Representative Plaintiff's and Class  
5 Members' PHI/PII and financial information is exacerbated by repeated warnings and alerts  
6 directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks  
7 in recent years.

8 55. The healthcare industry in particular has experienced a large number of high-profile  
9 cyberattacks even in just the short period preceding the filing of this Complaint and cyberattacks,  
10 generally, have become increasingly more common. More healthcare data breaches were reported  
11 in 2020 than in any other year, showing a 25% increase.<sup>6</sup> Additionally, according to the HIPAA  
12 Journal, the largest healthcare data breaches have been reported beginning in April 2021.<sup>7</sup>

13 56. For example, Universal Health Services experienced a cyberattack on September  
14 29, 2020 that appears similar to the attack on Defendant. As a result of this attack, Universal Health  
15 Services suffered a four-week outage of its systems which caused as much as \$67 million in  
16 recovery costs and lost revenue.<sup>8</sup> Similarly, in 2021, Scripps Health suffered a cyberattack, an  
17 event which effectively shut down critical health care services for a month and left numerous  
18 patients unable to speak to its physicians or access vital medical and prescription records.<sup>9</sup> A few  
19 months later, University of San Diego Health suffered a similar attack.<sup>10</sup>

20 57. Due to the high-profile nature of these breaches, and other breaches of its kind,  
21 Defendant was and/or certainly should have been on notice and aware of such attacks occurring in  
22 the healthcare industry and, therefore, should have assumed and adequately performed the duty of  
23

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

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

26 <sup>8</sup> [https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-  
reports-2020-fourth-quarter-and](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>9</sup> [https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-  
internal-systems-hit-by-cyberattack-2/2619540/](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>10</sup> [https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-  
employee-email-accounts-impacted/2670302/](https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-accounts-impacted/2670302/) (last accessed November 5, 2021).

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

1 preparing for such an imminent attack. This is especially true given that Defendant is a large,  
2 sophisticated operation with the resources to put adequate data security protocols in place.

3 58. Yet, despite the prevalence of public announcements of data breach and data  
4 security compromises, Defendant failed to take appropriate steps to protect Representative  
5 Plaintiff’s and Class Members’ PHI/PII and financial information from being compromised.

6

7 **Defendant Had an Obligation to Protect the Stolen Information**

8 59. Defendant’s failure to adequately secure Representative Plaintiff’s and Class  
9 Members’ sensitive data breaches duties it owes Representative Plaintiff and Class Members under  
10 statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to  
11 keep patients’ Protected Health Information private. As a covered entity, Defendant has a statutory  
12 duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiff’s and  
13 Class Members’ data. Moreover, Representative Plaintiff and Class Members surrendered their  
14 highly sensitive personal data to Defendant under the implied condition that Defendant would keep  
15 it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data,  
16 independent of any statute.

17 60. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to  
18 comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E  
19 (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule  
20 (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R.  
21 Part 160 and Part 164, Subparts A and C.

22 61. HIPAA’s Privacy Rule or Standards for Privacy of Individually Identifiable Health  
23 Information establishes national standards for the protection of health information.

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

27

28

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

1           63. HIPAA requires Defendant to “comply with the applicable standards,  
2 implementation specifications, and requirements” of HIPAA “with respect to electronic protected  
3 health information.” 45 C.F.R. § 164.302.

4           64. “Electronic protected health information” is “individually identifiable health  
5 information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45  
6 C.F.R. § 160.103.

- 7           65. HIPAA’s Security Rule requires Defendant to do the following:
- 8           a. Ensure the confidentiality, integrity, and availability of all electronic protected  
9 health information the covered entity or business associate creates, receives,  
maintains, or transmits;
  - 10           b. Protect against any reasonably anticipated threats or hazards to the security or  
11 integrity of such information;
  - 12           c. Protect against any reasonably anticipated uses or disclosures of such  
information that are not permitted; and
  - 13           d. Ensure compliance by its workforce.

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

20           67. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414,  
21 requires Defendant to provide notice of the Data Breach to each affected individual “without  
22 unreasonable delay and in no case later than 60 days following discovery of the breach.”  
23

24           68. Defendant was also prohibited by the Federal Trade Commission Act (the “FTC  
25 Act”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting  
26 commerce.” The Federal Trade Commission (the “FTC”) has concluded that a company’s failure  
27 to maintain reasonable and appropriate data security for consumers’ sensitive personal information  
28



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

1 is an “unfair practice” in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*,  
2 799 F.3d 236 (3d Cir. 2015).

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

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

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

18 72. Defendant owed a duty to Representative Plaintiff and Class Members to  
19 implement processes that would immediately detect a breach on its data security systems in a  
20 timely manner.

21 73. Defendant owed a duty to Representative Plaintiff and Class Members to act upon  
22 data security warnings and alerts in a timely fashion.

23 74. Defendant owed a duty to Representative Plaintiff and Class Members to disclose  
24 if its computer systems and data security practices were inadequate to safeguard individuals’  
25 PHI/PII and/or financial information from theft because such an inadequacy would be a material  
26 fact in the decision to entrust this PHI/PII and/or financial information to Defendants.

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



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

1           76. Defendant owed a duty to Representative Plaintiff and Class Members to encrypt  
2 and/or more reliably encrypt Representative Plaintiff’s and Class Members’ PHI/PII and financial  
3 information and monitor user behavior and activity in order to identify possible threats.  
4

5           **Value of the Relevant Sensitive Information**

6           77. While the greater efficiency of electronic health records translates to cost savings  
7 for providers, it also comes with the risk of privacy breaches. These electronic health records  
8 contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX’s,  
9 treatment plans) that is valuable to cyber criminals. One patient’s complete record can be sold for  
10 hundreds of dollars on the dark web. As such, PHI/PII and financial information are valuable  
11 commodities for which a “cyber black market” exists in which criminals openly post stolen  
12 payment card numbers, Social Security numbers, and other personal information on a number of  
13 underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and  
14 acutely affected by cyberattacks.

15           78. The high value of PHI/PII and financial information to criminals is further  
16 evidenced by the prices they will pay through the dark web. Numerous sources cite dark web  
17 pricing for stolen identity credentials. For example, personal information can be sold at a price  
18 ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.<sup>11</sup> Experian reports  
19 that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.<sup>12</sup> Criminals can  
20 also purchase access to entire company data breaches from \$999 to \$4,995.<sup>13</sup>

21           79. Between 2005 and 2019, at least 249 million people were affected by health care  
22 data breaches.<sup>14</sup> Indeed, during 2019 alone, over 41 million healthcare records were exposed,  
23

24 <sup>11</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).

25 <sup>12</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).

26 <sup>13</sup> *In the Dark*, VPNOverview, 2019, available at:  
27 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed January 21,  
2022).

28 <sup>14</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133> (last  
accessed January 21, 2022).

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

1 | stolen, or unlawfully disclosed in 505 data breaches.<sup>15</sup> In short, these sorts of data breaches are  
2 | increasingly common, especially among healthcare systems, which account for 30.03% of overall  
3 | health data breaches, according to cybersecurity firm Tenable.<sup>16</sup>

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

10 |       81. The FTC defines identity theft as “a fraud committed or attempted using the  
11 | identifying information of another person without authority.” The FTC describes “identifying  
12 | information” as “any name or number that may be used, alone or in conjunction with any other  
13 | information, to identify a specific person,” including, among other things, “[n]ame, Social Security  
14 | number, date of birth, official State or government issued driver’s license or identification number,  
15 | alien registration number, government passport number, employer or taxpayer identification  
16 | number.”

17 |       82. Identity thieves can use PHI/PII and financial information, such as that of  
18 | Representative Plaintiff and Class Members which Defendant failed to keep secure, to perpetrate  
19 | a variety of crimes that harm victims. For instance, identity thieves may commit various types of  
20 | government fraud such as immigration fraud, obtaining a driver’s license or identification card in  
21 | the victim’s name but with another’s picture, using the victim’s information to obtain government  
22 | benefits, or filing a fraudulent tax return using the victim’s information to obtain a fraudulent  
23 | refund.

24 |       83. The ramifications of Defendant’s failure to keep secure Representative Plaintiff’s  
25 | and Class Members’ PHI/PII and financial information are long lasting and severe. Once PHI/PII  
26 |

27 | <sup>15</sup> <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed  
28 | January 21, 2022).

<sup>16</sup> <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches> (last accessed January 21, 2022).

1 and financial information is stolen, particularly identification numbers, fraudulent use of that  
 2 information and damage to victims may continue for years. Indeed, the PHI/PII and/or financial  
 3 information of Representative Plaintiff and Class Members was taken by hackers to engage in  
 4 identity theft or to sell it to other criminals who will purchase the PHI/PII and/or financial  
 5 information for that purpose. The fraudulent activity resulting from the Data Breach may not come  
 6 to light for years.

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

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

16 85. The harm to Representative Plaintiff and Class Members is especially acute given  
 17 the nature of the leaked data. Medical identity theft is one of the most common, most expensive,  
 18 and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, “medical-  
 19 related identity theft accounted for 43 percent of all identity thefts reported in the United States in  
 20 2013,” which is more than identity thefts involving banking and finance, the government and the  
 21 military, or education.<sup>18</sup>

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

26  
 27 <sup>17</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).

28 <sup>18</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).

<sup>19</sup> *Id.*

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

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

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

10 89. And data breaches are preventable.<sup>22</sup> As Lucy Thompson wrote in the DATA  
11 BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could  
12 have been prevented by proper planning and the correct design and implementation of appropriate  
13 security solutions.”<sup>23</sup> he added that “[o]rganizations that collect, use, store, and share sensitive  
14 personal data must accept responsibility for protecting the information and ensuring that it is not  
15 compromised . . . .”<sup>24</sup>

16 90. Most of the reported data breaches are a result of lax security and the failure to  
17 create or enforce appropriate security policies, rules, and procedures ... Appropriate information  
18 security controls, including encryption, must be implemented and enforced in a rigorous and  
19 disciplined manner so that a *data breach never occurs*.<sup>25</sup>

20 91. Here, Defendant knew of the importance of safeguarding PHI/PII and financial  
21 information and of the foreseeable consequences that would occur if Representative Plaintiff’s and  
22 Class Members’ PHI/PII and financial information was stolen, including the significant costs that

23 \_\_\_\_\_  
24 <sup>20</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).

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

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

28 <sup>23</sup> *Id.* at 17.

<sup>24</sup> *Id.* at 28.

<sup>25</sup> *Id.*

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

1 would be placed on Representative Plaintiff and Class Members as a result of a breach of this  
2 magnitude. As detailed above, Defendant is a large, sophisticated organization with the resources  
3 to deploy robust cybersecurity protocols. It knew, or should have known, that the development and  
4 use of such protocols were necessary to fulfill its statutory and common law duties to  
5 Representative Plaintiff and Class Members. Its failure to do so is, therefore, intentional, willful,  
6 reckless, and/or grossly negligent.

7 92. Defendant disregarded the rights of Representative Plaintiff and Class Members by,  
8 *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and  
9 reasonable measures to ensure that its network servers were protected against unauthorized  
10 intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and  
11 training practices in place to adequately safeguard Representative Plaintiff's and Class Members'  
12 PHI/PII and/or financial information; (iii) failing to take standard and reasonably available steps  
13 to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an  
14 unreasonable duration of time; and (v) failing to provide Representative Plaintiff and Class  
15 Members prompt and accurate notice of the Data Breach.

16  
17 **FIRST CLAIM FOR RELIEF**  
18 **Negligence**  
19 **(On behalf of the Nationwide Class)**

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

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

27 95. Among these duties, Defendant were expected:  
28 a. to exercise reasonable care in obtaining, retaining, securing, safeguarding,  
deleting and protecting the PHI/PII and financial information in its  
possession;

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

- b. to protect Representative Plaintiff’s and Class Members’ PHI/PII and financial information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;
- c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and
- d. to promptly notify Representative Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected its PHI/PII and financial information.

96. Defendant knew that the PHI/PII and financial information was private and 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.

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

98. 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.

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

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

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

102. Representative Plaintiff’s and Class Members’ willingness to entrust Defendant with its PHI/PII and financial information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its

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

1 systems and the PHI/PII and financial information they stored on them from attack. Thus,  
2 Defendant had a special relationship with Representative Plaintiff and Class Members.

3 103. Defendant also had independent duties under state and federal laws that required  
4 Defendant to reasonably safeguard Representative Plaintiff’s and Class Members’ PHI/PII and  
5 financial information and promptly notify them about the Data Breach. These “independent duties”  
6 are untethered to any contract between Defendant and Representative Plaintiff and/or the  
7 remaining Class Members.

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

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



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

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

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

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

11           108. Defendant breached its duty to notify Representative Plaintiff and Class Members  
12 of the unauthorized access by waiting months after learning of the Data Breach to notify  
13 Representative Plaintiff and Class Members and then by failing and continuing to fail to provide  
14 Representative Plaintiff and Class Members sufficient information regarding the breach. To date,  
15 Defendant has not provided sufficient information to Representative Plaintiff and Class Members  
16 regarding the extent of the unauthorized access and continues to breach its disclosure obligations  
17 to Representative Plaintiff and Class Members.

18           109. Further, through its failure to provide timely and clear notification of the Data  
19 Breach to Representative Plaintiff and Class Members, Defendant prevented Representative  
20 Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI/PII and  
21 financial information, and to access their medical records and histories.

22           110. There is a close causal connection between Defendant’s failure to implement  
23 security measures to protect the PHI/PII and financial information of Representative Plaintiff and  
24 Class Members and the harm suffered, or risk of imminent harm suffered by Representative  
25 Plaintiff and Class Members. Representative Plaintiff’s and Class Members’ PHI/PII and financial  
26 information was accessed as the proximate result of Defendant’s failure to exercise reasonable  
27 care in safeguarding such PHI/PII and financial information by adopting, implementing, and  
28 maintaining appropriate security measures.



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

1           111. Defendant’s wrongful actions, inactions, and omissions constituted (and continue  
2 to constitute) common law negligence.

3           112. The damages Representative Plaintiff and Class Members have suffered (as alleged  
4 above) and will suffer were and are the direct and proximate result of Defendant’s grossly  
5 negligent conduct.

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

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

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

19           116. As a direct and proximate result of Defendant’s negligence and negligence *per se*,  
20 Representative Plaintiff and Class Members have suffered and will suffer injury, including but not  
21 limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PHI/PII and financial  
22 information is used; (iii) the compromise, publication, and/or theft of their PHI/PII and financial  
23 information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery  
24 from identity theft, tax fraud, and/or unauthorized use of their PHI/PII and financial information;  
25 (v) lost opportunity costs associated with effort expended and the loss of productivity addressing  
26 and attempting to mitigate the actual and future consequences of the Data Breach, including but  
27 not limited to, efforts spent researching how to prevent, detect, contest, and recover from  
28 embarrassment and identity theft; (vi) lost continuity in relation to its healthcare; (vii) the

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

1 continued risk to its PHI/PII and financial information, which may remain in Defendant’s  
2 possession and is subject to further unauthorized disclosures so long as Defendant fails to  
3 undertake appropriate and adequate measures to protect Representative Plaintiff’s and Class  
4 Members’ PHI/PII and financial information in its continued possession; and (viii) future costs in  
5 terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the  
6 impact of the PHI/PII and financial information compromised as a result of the Data Breach for  
7 the remainder of the lives of Representative Plaintiff and Class Members.

8 117. As a direct and proximate result of Defendant’s negligence and negligence *per se*,  
9 Representative Plaintiff and Class Members have suffered and will continue to suffer other forms  
10 of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy,  
11 and other economic and non-economic losses.

12 118. Additionally, as a direct and proximate result of Defendant’s negligence and  
13 negligence *per se*, Representative Plaintiff and Class Members have suffered and will suffer the  
14 continued risks of exposure of their PHI/PII and financial information, which remain in  
15 Defendant’s possession and are subject to further unauthorized disclosures so long as Defendant  
16 fails to undertake appropriate and adequate measures to protect the PHI/PII and financial  
17 information in its continued possession.

18  
19 **SECOND CLAIM FOR RELIEF**  
20 **Invasion of Privacy**  
21 **(On behalf of the Nationwide Class)**

22 119. 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.

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

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

122. Defendant failed to protect and released to unknown and unauthorized third parties  
the PHI/PII and financial information 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            123. 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            124. 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            125. 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            126. 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            127. 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            128. 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            129. 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            130. 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 **THIRD CLAIM FOR RELIEF**  
8 **Breach of Implied Contract**  
9 **(On behalf of the Nationwide Class)**

10 131. 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.

12 132. 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.

16 133. 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.

19 134. 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.

23 135. 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           136. 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           137. Representative Plaintiff and Class Members fully performed their obligations under  
5 the implied contracts with Defendant.

6           138. 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           139. 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  
19                           **FOURTH CLAIM FOR RELIEF**  
20                           **Unjust Enrichment**  
21                           **(On behalf of the Nationwide Class)**

22           140. 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           141. By its wrongful acts and omissions described herein, Defendant has obtained a  
25 benefit by unduly taking advantage of Representative Plaintiff and Class Members.

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

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

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

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

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

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

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

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

27  
28

**RELIEF SOUGHT**

**WHEREFORE**, Representative Plaintiff, on behalf of herself and each member of the proposed National Class and the Indiana 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 Indiana 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 e. requiring Defendant to engage independent third-party security auditors and  
2 internal personnel to run automated security monitoring, simulated attacks,  
3 penetration tests, and audits on Defendant’s systems on a periodic basis;
- 4 f. prohibiting Defendant from maintaining Representative Plaintiff’s and  
5 Class Members’ PII/PHI on a cloud-based database;
- 6 g. requiring Defendant to segment data by creating firewalls and access  
7 controls so that, if one area of Defendant’s network is compromised,  
8 hackers cannot gain access to other portions of Defendant’s systems;
- 9 h. requiring Defendant to conduct regular database scanning and securing  
10 checks;
- 11 i. requiring Defendant to establish an information security training program  
12 that includes at least annual information security training for all employees,  
13 with additional training to be provided as appropriate based upon the  
14 employees’ respective responsibilities with handling PII/PHI, as well as  
15 protecting the PII/PHI of Representative Plaintiff and Class Members;
- 16 j. requiring Defendant to implement a system of tests to assess its respective  
17 employees’ knowledge of the education programs discussed in the  
18 preceding subparagraphs, as well as randomly and periodically testing  
19 employees’ compliance with Defendant’s policies, programs, and systems  
20 for protecting personal identifying information;
- 21 k. requiring Defendant to implement, maintain, review, and revise as  
22 necessary a threat management program to appropriately monitor  
23 Defendant’s networks for internal and external threats, and assess whether  
24 monitoring tools are properly configured, tested, and updated;
- 25 l. requiring Defendant to meaningfully educate all Class Members about the  
26 threats that they face as a result of the loss of its confidential personal  
27 identifying information to third parties, as well as the steps affected  
28 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: August 26, 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