

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

1 Laura Van Note, Esq. (S.B. #310160)\*  
2 **COLE & VAN NOTE**  
3 555 12<sup>th</sup> Street, Suite 2100  
4 Oakland, California 94607  
5 Telephone: (510) 891-9800  
6 Facsimile: (510) 891-7030  
7 Email: lvn@colevannote.com  
8 Web: www.colevannote.com

6 David Hilton Wise, Esq.  
7 Nevada Bar No. 11014  
8 **WISE LAW FIRM, PLC**  
9 421 Court Street  
10 Reno, Nevada, 89501  
11 Telephone: (775) 329-1766  
12 Facsimile: (703) 934-6377  
13 Email: dwise@wiselaw.pro

14 \* *Pro hac vice* forthcoming

15 Attorneys for Representative Plaintiff  
16 and the Plaintiff Class

17 **UNITED STATES DISTRICT COURT**  
18 **DISTRICT OF NEVADA**

17 KEVIN O’ROURKE, individually, and on  
18 behalf of all others similarly situated,  
19 Plaintiff,  
20 v.  
21 NORTHWELL HEALTH, INC. and  
22 PERRY JOHNSON & ASSOCIATES,  
23 INC.,  
24 Defendants.

25 **Case No.**  
26 **CLASS ACTION**  
27 **COMPLAINT**

28 **[JURY TRIAL DEMANDED]**

29 **INTRODUCTION**

30 1. Representative Plaintiff Kevin O’Rourke (“Representative Plaintiff”) brings this  
31 class action against Defendant Northwell Health, Inc. (or “Northwell”) and Defendant Perry  
32 Johnson & Associates (or “PJ&A”) (collectively “Defendant”) for its failure to properly secure

1 and safeguard Representative Plaintiff’s and Class Members’ protected health information and  
 2 personally identifiable information stored within Defendant’s information network, including  
 3 without limitation, names, dates of birth, addresses, medical record numbers, hospital account  
 4 numbers and clinical information such as the name of patients’ treatment facility, the name of  
 5 patients’ healthcare provider, admission diagnoses and times of service (these types of  
 6 information, *inter alia*, being thereafter referred to, collectively, as “protected health information”  
 7 or “PHI”<sup>1</sup> and “personally identifiable information” or “PII”).<sup>2</sup>

8 2. With this action, Representative Plaintiff seeks to hold Defendant responsible for  
 9 the harms it caused and will continue to cause Representative Plaintiff and, at least, 1.2 million<sup>3</sup>  
 10 other similarly situated persons in the massive and preventable cyberattack purportedly discovered  
 11 by Defendant on May 2, 2023, by which cybercriminals infiltrated Defendant’s inadequately  
 12 protected network servers and accessed highly sensitive PHI/PII which was being kept unprotected  
 13 (the “Data Breach”).

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

19 4. While Defendant claims to have discovered the breach as early as May 2, 2023,  
 20 Defendant did not begin informing victims of the Data Breach until November 3, 2023. Indeed,

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

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

<sup>3</sup> “Millions of Northwell Health patients potentially caught in transcription data breach,”  
*Becker’s Health It*, <https://www.beckershospitalreview.com/cybersecurity/millions-of-northwell-health-patients-potentially-caught-in-transcription-data-breach.html/> (last accessed November 13,  
 2023).

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

1 Representative Plaintiff and Class Members were wholly unaware of the Data Breach until they  
2 received letters from Defendant informing them of it. The Notice received by Representative  
3 Plaintiff was dated November 3, 2023.

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

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

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

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

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

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

12  
13 **JURISDICTION AND VENUE**

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

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

21 12. Defendant routinely conducts business in the State where this District is located,  
22 has sufficient minimum contacts in this State and has intentionally availed itself of this jurisdiction  
23 by marketing and selling products and services, and by accepting and processing payments for  
24 those products and services within this State.

25 13. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of  
26 the events that gave rise to Representative Plaintiff's claims took place within this District, and  
27 Defendant does business in this Judicial District.

28

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

**PLAINTIFF**

1  
2 14. Representative Plaintiff is an adult individual, and, at all relevant times herein, was  
3 a resident and citizen of the State of New York. Representative Plaintiff is a victim of the Data  
4 Breach.

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

9 16. At all times herein relevant, Representative Plaintiff is and was a member of each  
10 of the Class.

11 17. As required in order to obtain services and/or employment from Defendant,  
12 Representative Plaintiff provided Defendant with highly sensitive PHI/PII.

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

16 19. Representative Plaintiff received a letter from Defendant, dated November 3, 2023,  
17 stating Representative Plaintiff's PHI/PII was involved in the Data Breach (the "Notice").

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

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

28

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

1 22. Representative Plaintiff suffered lost time, annoyance, interference and  
2 inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss  
3 of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling  
4 Representative Plaintiff’s PHI/PII.

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

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

12  
13 **DEFENDANTS**

14 25. Defendant Northwell Health, Inc. is a New York not-for-profit corporation with a  
15 principal place of business located at 2000 Marcus Ave., New Hyde Park, New York 11042.  
16 Defendant is “the largest health system in New York.”<sup>4</sup>

17 26. Defendant Perry Johnson & Associates is a Nevada corporation with a principal  
18 place of business located at 1489 W. Warm Springs Rd., Henderson, Nevada 89014. Defendant is  
19 a transcription service that claims its “expertise in health/legal information technology industries  
20 enables [it] to help meet [clients] meet those demands while maintaining profitability.”<sup>5</sup>

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

26  
27  
28 <sup>4</sup> “About Northwell,” *Northwell Health*, <https://www.northwell.edu/about-northwell/> (last accessed November 13, 2023).

<sup>5</sup> “About PJ&A,” *PJ&A*, <https://www.pjats.com/about-pja/> (last accessed November 13, 2023).

**CLASS ACTION ALLEGATIONS**

28. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of Representative Plaintiff and the following class (the “Class”):

**Nationwide Class:**

“All individuals within the United States of America whose PHI/PII was exposed to unauthorized third parties as a result of the data breach allegedly discovered by Defendant on May 2, 2023.”

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

30. In the alternative, Representative Plaintiff requests additional subclasses as necessary based on the types of PHI/PII that were compromised.

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

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

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Class are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff is informed and believe and, on that basis, alleges that the total number of Class Members is in the millions of individuals. Membership in the Class will be determined by analysis of Defendant’s records.

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

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

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

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

- 1) Whether Defendant had a legal duty to Representative Plaintiff and the Class to exercise due care in collecting, storing, using and/or safeguarding their PHI/PII;
- 2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;
- 3) Whether Defendant’s security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;
- 4) Whether Defendant’s failure to implement adequate data security measures allowed the Data Breach to occur;
- 5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;
- 6) Whether Defendant adequately, promptly and accurately informed Representative Plaintiff and Class Members that their PHI/PII had been compromised;
- 7) How and when Defendant actually learned of the Data Breach;
- 8) Whether Defendant’s conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Representative Plaintiff’s and Class Members’ PHI/PII;
- 9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- 10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiff’s and Class Members’ PHI/PII;
- 11) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant’s wrongful conduct; and
- 12) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant’s wrongful conduct.

c. Typicality: Representative Plaintiff’s claims are typical of the claims of the Plaintiff Class. Representative Plaintiff and all members of the Plaintiff Class sustained damages arising out of and caused by Defendant’s common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiff in this class action is an adequate representative of the Plaintiff Class in that the Representative Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the



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

1 Class in its entirety. Representative Plaintiff anticipates no management  
2 difficulties in this litigation.

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

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

18 34. This class action is also appropriate for certification because Defendant has acted  
19 or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's  
20 imposition of uniform relief to ensure compatible standards of conduct toward the Class Members  
21 and making final injunctive relief appropriate with respect to the Class in its entirety. Defendant's  
22 policies and practices challenged herein apply to and affect Class Members uniformly and  
23 Representative Plaintiff's challenge of these policies and practices hinges on Defendant's conduct  
24 with respect to the Class in its entirety, not on facts or law applicable only to Representative  
25 Plaintiff.

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

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

1 **COMMON FACTUAL ALLEGATIONS**

2 **The Cyberattack**

3 37. In the course of the Data Breach, one or more unauthorized third parties accessed  
4 Class Members' sensitive data, including but not limited to, names, dates of birth, addresses,  
5 medical record numbers, hospital account numbers and clinical information such as the name of  
6 patients' treatment facility, the name of patients' healthcare provider, admission diagnoses and  
7 times of service. Representative Plaintiff was among the individuals whose data was accessed in  
8 the Data Breach.

9 38. Representative Plaintiff was provided the information detailed above upon  
10 Representative Plaintiff's receipt of a letter from Defendant, dated November 3, 2023.  
11 Representative Plaintiff was not aware of the Data Breach until receiving that letter.  
12

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

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

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

21 41. The Notice included, *inter alia*, the claims that Defendant had learned of the Data  
22 Breach on May 2, 2023, and Defendant later discovered the unauthorized access began as early as  
23 April 7, 2023.

24 42. Defendant had and continues to have obligations created by HIPAA, applicable  
25 federal and state law as set forth herein, reasonable industry standards, common law and its own  
26 assurances and representations to keep Representative Plaintiff's and Class Members' PHI/PII  
27 confidential and to protect such PHI/PII from unauthorized access.  
28

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

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

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

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

19  
20 **Defendant Collected/Stored Class Members' PHI/PII**

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

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

27           48. By obtaining, collecting and storing Representative Plaintiff's and Class Members'  
28 PHI/PII, Defendant assumed legal and equitable duties over the PHI/PII and knew or should have

1 known that it was thereafter responsible for protecting Representative Plaintiff's and Class  
2 Members' PHI/PII from unauthorized disclosure.

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

7 50. Defendant could have prevented the Data Breach, which began no later than April  
8 7, 2023, by properly securing and encrypting and/or more securely encrypting its servers generally,  
9 as well as Representative Plaintiff's and Class Members' PHI/PII.

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

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

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

21  
22 **Defendant Had an Obligation to Protect the Stolen Information**

23 54. In failing to adequately secure Representative Plaintiff's and Class Member's  
24 sensitive data, Defendant breached duties it owed Representative Plaintiff and Class Members  
25 under statutory and common law. Under HIPAA, health insurance providers have an affirmative  
26 duty to keep patients' PHI/PII confidential. As a covered entity, Defendant has a statutory duty  
27 under HIPAA and other federal and state statutes to safeguard Representative Plaintiff's and Class  
28 Members' PHI/PII. Moreover, Representative Plaintiff and Class Members surrendered their

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

1 highly sensitive PHI/PII to Defendant under the implied condition that Defendant would keep it  
2 private and secure. Accordingly, Defendant also has an implied duty to safeguard their PHI/PII,  
3 independent of any statute.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 credentials. For example, personal information can be sold at a price ranging from \$40 to \$200,  
 2 and bank details have a price range of \$50 to \$200.<sup>6</sup> Experian reports that a stolen credit or debit  
 3 card number can sell for \$5 to \$110 on the dark web.<sup>7</sup> Criminals can also purchase access to entire  
 4 company data breaches from \$999 to \$4,995.<sup>8</sup>

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

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

16 76. The FTC defines identity theft as “a fraud committed or attempted using the  
 17 identifying information of another person without authority.” The FTC describes “identifying  
 18 information” as “any name or number that may be used, alone or in conjunction with any other  
 19 information, to identify a specific person,” including, among other things, “[n]ame, Social Security  
 20 number, date of birth, official State or government issued driver’s license or identification number,  
 21

22 <sup>6</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct.  
 23 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed November 13, 2023).

24 <sup>7</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.  
 25 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 13, 2023).

26 <sup>8</sup> *In the Dark*, VPNOverview, 2019, available at:  
 27 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed November 13,  
 28 2023).

<sup>9</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/> (last  
 accessed November 13, 2023).

<sup>10</sup> <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed  
 November 13, 2023).

<sup>11</sup> <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/> (last accessed November 13, 2023).



1 alien registration number, government passport number, employer or taxpayer identification  
 2 number.”

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

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

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

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

23 80. The harm to Representative Plaintiff and Class Members is especially acute given  
 24 the nature of the leaked data. Medical identity theft is one of the most common, most expensive  
 25 and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, “medical-  
 26 related identity theft accounted for 43 percent of all identity thefts reported in the United States in  
 27

28 <sup>12</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:  
<http://www.gao.gov/new.items/d07737.pdf> (last accessed November 13, 2023).

1 2013,” which is more than identity thefts involving banking and finance, the government and the  
 2 military, or education.<sup>13</sup>

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

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

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

16 84. And data breaches are preventable.<sup>17</sup> As Lucy Thompson wrote in the DATA  
 17 BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could  
 18 have been prevented by proper planning and the correct design and implementation of appropriate  
 19 security solutions.”<sup>18</sup> She added that “[o]rganizations that collect, use, store, and share sensitive  
 20 personal data must accept responsibility for protecting the information and ensuring that it is not  
 21 compromised....”<sup>19</sup>

22  
 23 <sup>13</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 November 13, 2023).

24 <sup>14</sup> *Id.*

25 <sup>15</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 November 13, 2023).

26 <sup>16</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 November 13, 2023).

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

<sup>18</sup> *Id.* at 17.

<sup>19</sup> *Id.* at 28.

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

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

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

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

21  
 22 **FIRST CLAIM FOR RELIEF**  
**Negligence**  
 23 **(On behalf of the Nationwide Class)**

24 88. Each and every allegation of the preceding paragraphs is incorporated in this Court  
 25 with the same force and effect as though fully set forth herein.

26 89. At all times herein relevant, Defendant owed Representative Plaintiff and Class  
 27 Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII  
 28

<sup>20</sup> *Id.*

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

1 and to use commercially reasonable methods to do so. Defendant took on this obligation upon  
2 accepting and storing Representative Plaintiff's and Class Members' PHI/PII on its computer  
3 systems and networks.

4 90. Among these duties, Defendant was expected:

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

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

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

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

22 94. Only Defendant was in the position to ensure that its systems and protocols were  
23 sufficient to protect the PHI/PII that Representative Plaintiff and Class Members had entrusted to  
24 it.

25 95. Defendant breached its duties to Representative Plaintiff and Class Members by  
26 failing to provide fair, reasonable or adequate computer systems and data security practices to  
27 safeguard Representative Plaintiff's and Class Members' PHI/PII.  
28

1           96. Because Defendant knew that a breach of its systems could damage millions of  
 2 individuals, including Representative Plaintiff and Class Members, Defendant had a duty to  
 3 adequately protect its data systems and the PHI/PII contained thereon.

4           97. Representative Plaintiff's and Class Members' willingness to entrust Defendant  
 5 with its PHI/PII was predicated on the understanding that Defendant would take adequate security  
 6 precautions. Moreover, only Defendant had the ability to protect its systems and the PHI/PII it  
 7 stored on them from attack. Thus, Defendant had a special relationship with Representative  
 8 Plaintiff and Class Members.

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

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

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

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

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

3           101. 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           102. The law further imposes an affirmative duty on Defendant to timely disclose the  
7 unauthorized access and theft of the PHI/PII to Representative Plaintiff and Class Members so that  
8 they could and/or still can take appropriate measures to mitigate damages, protect against adverse  
9 consequences and thwart future misuse of their PHI/PII.

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

17           104. Further, through its failure to provide timely and clear notification of the Data  
18 Breach to Representative Plaintiff and Class Members, Defendant prevented Representative  
19 Plaintiff and Class Members from taking meaningful, proactive steps to, *inter alia*, secure and/or  
20 access their PHI/PII.

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

27           106. Defendant’s wrongful actions, inactions and omissions constituted (and continue to  
28 constitute) common law negligence.

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

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

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

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

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

16           111. As a direct and proximate result of Defendant’s negligence and negligence *per se*,  
17 Representative Plaintiff and Class Members have suffered and will continue to suffer injury,  
18 including but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their  
19 PHI/PII is used, (iii) the compromise, publication and/or theft of their PHI/PII, (iv) out-of-pocket  
20 expenses associated with the prevention, detection and recovery from identity theft, tax fraud  
21 and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with effort expended  
22 and the loss of productivity addressing and attempting to mitigate the actual and future  
23 consequences of the Data Breach, including but not limited to efforts spent researching how to  
24 prevent, detect, contest and recover from embarrassment and identity theft, (vi) lost continuity in  
25 relation to their personal records, (vii) the continued risk to their PHI/PII, which may remain in  
26 Defendant’s possession and is subject to further unauthorized disclosures so long as Defendant  
27 fails to undertake appropriate and adequate measures to protect Representative Plaintiff’s and  
28 Class Members’ PHI/PII in its continued possession, and (viii) future costs in terms of time, effort

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

1 and money that will be expended to prevent, detect, contest and repair the impact of the PHI/PII  
2 compromised as a result of the Data Breach for the remainder of the lives of Representative  
3 Plaintiff and Class Members.

4 112. As a direct and proximate result of Defendant’s negligence and negligence *per se*,  
5 Representative Plaintiff and Class Members have suffered and will continue to suffer other forms  
6 of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy and  
7 other economic and noneconomic losses.

8 113. Additionally, as a direct and proximate result of Defendant’s negligence and  
9 negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to  
10 suffer the continued risks of exposure of their PHI/PII, which remains in Defendant’s possession  
11 and is subject to further unauthorized disclosures so long as Defendant fails to undertake  
12 appropriate and adequate measures to protect PHI/PII in its continued possession.

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

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

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

21 116. Defendant required Representative Plaintiff and Class Members to provide and  
22 entrust their PHI/PII as a condition of obtaining Defendant’s services from Defendant.

23 117. Defendant solicited and invited Representative Plaintiff and Class Members to  
24 provide their PHI/PII as part of Defendant’s regular business practices. Representative Plaintiff  
25 and Class Members accepted Defendant’s offers and provided their PHI/PII to Defendant.

26 118. As a condition of being direct customers and/or employees of Defendant,  
27 Representative Plaintiff and Class Members provided and entrusted their PHI/PII to Defendant. In  
28 so doing, Representative Plaintiff and Class Members entered into implied contracts with



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

1 Defendant by which Defendant agreed to safeguard and protect such non-public information, to  
2 keep such information secure and confidential and to timely and accurately notify Representative  
3 Plaintiff and Class Members if its data had been breached and compromised or stolen.

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

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

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

12 122. As a direct and proximate result of Defendant's above-described breach of implied  
13 contract, Representative Plaintiff and Class Members have suffered and will continue to suffer (i)  
14 ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in  
15 monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in  
16 monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data,  
17 (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (vi) other  
18 economic and noneconomic harm.

19  
20 **THIRD CLAIM FOR RELIEF**  
21 **Breach of the Implied Covenant of Good Faith and Fair Dealing**  
22 **(On behalf of the Nationwide Class)**

23 123. Each and every allegation of the preceding paragraphs is incorporated in this Count  
24 with the same force and effect as though fully set forth therein.

25 124. Every contract in this State has an implied covenant of good faith and fair  
26 dealing. This implied covenant is an independent duty and may be breached even when there  
27 is no breach of a contract's actual and/or express terms.

28 125. Representative Plaintiff and Class Members have complied with and performed all  
conditions of their contracts with Defendant.

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

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

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

### **RELIEF SOUGHT**

10  
11  
12           **WHEREFORE**, Representative Plaintiff, on Representative Plaintiff’s own behalf and on  
13 behalf of each member of the proposed National Class, respectfully requests that the Court enter  
14 judgment in favor of Representative Plaintiff and the Class and for the following specific relief  
15 against Defendant as follows:

16           1. That the Court declare, adjudge and decree that this action is a proper class action  
17 and certify the proposed Class and/or any other appropriate Subclasses under Federal Rules of  
18 Civil Procedure Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative  
19 Plaintiff’s counsel as Class Counsel;

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

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

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

28

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

- 1           5.       For injunctive relief requested by Representative Plaintiff, including but not limited  
 2 to injunctive and other equitable relief as is necessary to protect the interests of Representative  
 3 Plaintiff and Class Members, including but not limited to an Order:
- 4           a.       prohibiting Defendant from engaging in the wrongful and unlawful acts  
 5 described herein;
- 6           b.       requiring Defendant to protect, including through encryption, all data  
 7 collected through the course of business in accordance with all applicable  
 8 regulations, industry standards and federal, state or local laws;
- 9           c.       requiring Defendant to delete and purge Representative Plaintiff’s and Class  
 10 Members’ PHI/PII unless Defendant can provide to the Court reasonable  
 11 justification for the retention and use of such information when weighed  
 12 against the privacy interests of Representative Plaintiff and Class Members;
- 13           d.       requiring Defendant to implement and maintain a comprehensive  
 14 Information Security Program designed to protect the confidentiality and  
 15 integrity of Representative Plaintiff’s and Class Members’ PHI/PII;
- 16           e.       requiring Defendant to engage independent third-party security auditors and  
 17 internal personnel to run automated security monitoring, simulated attacks,  
 18 penetration tests and audits on Defendant’s systems on a periodic basis;
- 19           f.       prohibiting Defendant from maintaining Representative Plaintiff’s and  
 20 Class Members’ PHI/PII on a cloud-based database;
- 21           g.       requiring Defendant to segment data by creating firewalls and access  
 22 controls so that if one area of Defendant’s network is compromised, hackers  
 23 cannot gain access to other portions of Defendant’s systems;
- 24           h.       requiring Defendant to conduct regular database scanning and securing  
 25 checks;
- 26           i.       requiring Defendant to establish an information security training program  
 27 that includes at least annual information security training for all employees,  
 28 with additional training to be provided as appropriate based upon the  
 employees’ respective responsibilities with handling PHI/PII, as well as  
 protecting the PHI/PII of Representative Plaintiff and Class Members;
- j.       requiring Defendant to implement a system of tests to assess its respective  
 employees’ knowledge of the education programs discussed in the  
 preceding subparagraphs, as well as randomly and periodically testing  
 employees’ compliance with Defendant’s policies, programs and systems  
 for protecting personal identifying information;
- k.       requiring Defendant to implement, maintain, review and revise as necessary  
 a threat management program to appropriately monitor Defendant’s  
 networks for internal and external threats, and assess whether monitoring  
 tools are properly configured, tested and updated; and
- l.       requiring Defendant to meaningfully educate all Class Members about the  
 threats that they face as a result of the loss of their confidential personal

1 identifying information to third parties, as well as the steps affected  
2 individuals must take to protect themselves.

3 6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

4 7. For an award of attorneys' fees, costs and litigation expenses, as allowed by law;

5 and

6 8. For all other Orders, findings and determinations identified and sought in this

7 Complaint.

8  
9 **JURY DEMAND**

10 Representative Plaintiff, individually and on behalf of the Plaintiff Class, hereby demands  
11 a trial by jury for all issues triable by jury.

12  
13 Dated: November 14, 2023

14 By: /s/ David Hilton Wise  
15 David Hilton Wise, Esq.  
16 Nevada Bar No. 11014  
17 **WISE LAW FIRM, PLC**  
18 421 Court Street  
19 Reno, Nevada, 89501  
20 Telephone: (775) 329-1766  
21 Facsimile: (703) 934-6377  
22 Email: [dwise@wiselaw.pro](mailto:dwise@wiselaw.pro)

23 Laura Van Note, Esq. (S.B. #310160)\*  
24 **COLE & VAN NOTE**  
25 555 12<sup>th</sup> Street, Suite 2100  
26 Oakland, California 94607  
27 Telephone: (510) 891-9800  
28 Facsimile: (510) 891-7030  
Email: [sec@colevannote.com](mailto:sec@colevannote.com)

*Attorneys for Representative Plaintiff and the Plaintiff Class*

*\*Pro hac vice forthcoming*

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