

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

7  
 8 Attorneys for Representative Plaintiff  
 and the Plaintiff Classes  
 9

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

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

13 VERONICA ROMAN, individually, and on  
 behalf of all others similarly situated,

14 Plaintiff,

15 vs.

16 HANES BRANDS, INC.,

17 Defendant.  
 18  
 19  
 20  
 21  
 22  
 23

**Case No.**

**CLASS ACTION**

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

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

**[JURY TRIAL DEMANDED]**

1 Representative Plaintiff alleges as follows:  
2

3 **INTRODUCTION**

4 1. Representative Plaintiff Veronica Roman (“Representative Plaintiff”) brings this  
5 class action against Defendant Hanes Brands, Inc. (“Defendant” or “Hanes”) for its failure to  
6 properly secure and safeguard Representative Plaintiff’s and Class Members’ personally  
7 identifiable information stored within Defendant’s information network, including, without  
8 limitation, dates of birth, financial account information, government issued identification numbers  
9 such as drivers’ license numbers, passport information, Social Security numbers, and other  
10 information related to benefits and employment, including certain limited health information  
11 provided for employment related purposes (these types of information, *inter alia*, being thereafter  
12 referred to, collectively, as “protected health information” or “PHI”<sup>1</sup> and “personally identifiable  
13 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 countless other similarly  
16 situated persons in the massive and preventable cyberattack purportedly discovered by Defendant  
17 on May 24, 2022, by which cybercriminals infiltrated Defendant’s inadequately protected network  
18 servers and accessed highly sensitive PHI/PII and financial information, which was being kept  
19 unprotected (the “Data Breach”).

20 3. While Defendant claims to have discovered the breach as early as May 24, 2022,  
21 Defendant did not begin informing victims of the Data Breach until August 2022 and failed to  
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 (“PHI/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. PHI/PII also is generally defined to include  
certain identifiers that do not on its face name an individual, but that are considered to be  
particularly sensitive and/or valuable if in the wrong hands (for example, Social Security  
numbers, passport numbers, driver’s license numbers, financial account numbers).

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

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

1 inform victims when or for how long the Data Breach occurred. Indeed, Representative Plaintiff  
2 and Class Members were wholly unaware of the Data Breach until they received letters from  
3 Defendant informing them of it. The notice received by Representative Plaintiff was dated  
4 September 30, 2022.

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

9 5. By obtaining, collecting, using, and deriving a benefit from Representative  
10 Plaintiff’s and Class Members’ PHI/PII, Defendant assumed legal and equitable duties to those  
11 individuals. These duties arise from state and federal statutes and regulations as well as common  
12 law principles.

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

24  
25 **JURISDICTION AND VENUE**

26 7. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction).  
27 Specifically, this Court has subject matter and diversity jurisdiction over this action under 28  
28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum

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

1 or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the  
2 proposed class, and at least one other Class Member is a citizen of a state different from Defendant.

3 8. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in  
4 this Court under 28 U.S.C. §1367.

5 9. Defendant is a citizen of North Carolina that routinely conducts business in the  
6 State where this district is located, has sufficient minimum contacts in this State, and has  
7 intentionally availed itself of this jurisdiction by marketing and selling products and services, and  
8 by accepting and processing payments for those products and services within this State.

9 10. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of  
10 the events that gave rise to Representative Plaintiff’s claims took place within this District, and  
11 Plaintiff is domiciled in this Judicial District.

12  
13 **PLAINTIFF**

14 11. Representative Plaintiff is an adult individual and, at all relevant times herein, a  
15 resident and citizen of the state of California. Representative Plaintiff is victims of the Data Breach.  
16 Representative Plaintiff was an employee of Defendant’s.

17 12. Defendant received highly sensitive personal and financial information from  
18 Representative Plaintiff in connection with Plaintiff’s employment. As a result, Representative  
19 Plaintiff’s information was among the data accessed by an unauthorized third-party in the Data  
20 Breach.

21 13. Representative Plaintiff received—and was a “consumer” for purposes of obtaining  
22 goods from Defendant within this state.

23 14. At all times herein relevant, Representative Plaintiff is and was a member of each  
24 of the Classes.

25 15. As required in order to obtain employment from Defendant, Representative  
26 Plaintiff provided Defendant with highly sensitive personal and financial information.

27 16. Representative Plaintiff’s PHI/PII was exposed in the Data Breach because  
28 Defendant stored and/or shared Representative Plaintiff’s PHI/PII and financial information. Her

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

1 PHI/PII and financial information was within the possession and control of Defendant at the time  
2 of the Data Breach.

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

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

11 19. Representative Plaintiff suffered lost time, annoyance, interference, and  
12 inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss  
13 of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling her  
14 PHI/PII and/or financial information.

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

19 21. Representative Plaintiff has a continuing interest in ensuring that her PHI/PII and  
20 financial information, which, upon information and belief, remains backed up in Defendant's  
21 possession, is protected and safeguarded from future breaches.

22  
23 **DEFENDANT**

24 22. Defendant is a Maryland corporation with a principal place of business located at  
25 1000 E. Hanes Mill Road Winston-Salem, North Carolina 27105.

26 23. Defendant produces and sells clothing. Defendant is domiciliary and citizen of the  
27 State of North Carolina.

28



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

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

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

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

- 16           1) Whether Defendant had a legal duty to Representative Plaintiff and the  
17 Classes to exercise due care in collecting, storing, using and/or  
18 safeguarding their PHI/PII;
- 19           2) Whether Defendant knew or should have known of the susceptibility  
20 of its data security systems to a data breach;
- 21           3) Whether Defendant's security procedures and practices to protect its  
22 systems was reasonable in light of the measures recommended by data  
23 security experts;
- 24           4) Whether Defendant's failure to implement adequate data security  
25 measures allowed the Data Breach to occur;
- 26           5) Whether Defendant failed to comply with its own policies and  
27 applicable laws, regulations, and industry standards relating to data  
28 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 the PHI/PII of Representative Plaintiff and Class Members;
- 9) Whether Defendant adequately addressed and fixed the vulnerabilities  
which permitted the Data Breach to occur;
- 10) Whether Defendant engaged in unfair, unlawful, or deceptive practices  
by failing to safeguard the PHI/PII of Representative Plaintiff and  
Class Members;

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

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

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 the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

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

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

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

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

8  
9 **COMMON FACTUAL ALLEGATIONS**

10 **The Cyberattack**

11 33. In the course of the Data Breach, one or more unauthorized third-parties accessed  
12 Class Members' sensitive data including, but not limited to, dates of birth, financial account  
13 information, government issued identification numbers such as drivers' license numbers, passport  
14 information, Social Security numbers, and other information related to benefits and employment,  
15 including certain limited health information provided for employment related purposes.  
16 Representative Plaintiff was among the individuals whose data was accessed in the Data Breach.

17 34. Representative Plaintiff was provided the information detailed above upon her  
18 receipt of a letter from Defendant, dated on or about September 30, 2022. Representative Plaintiff  
19 was not aware of the Data Breach—or even that Defendant was still in possession of her data until  
20 receiving that letter.

21  
22 **Defendant's Failed Response to the Breach**

23 35. Upon information and belief, the unauthorized third-party cybercriminals gained  
24 access to Representative Plaintiff's and Class Members' PHI/PII and financial information with  
25 the intent of engaging in misuse of the PHI/PII and financial information, including marketing and  
26 selling Representative Plaintiff's and Class Members' PHI/PII.

27 36. Not until roughly three months after it claims to have discovered the Data Breach  
28 did Defendant begin sending the Notice to persons whose PHI/PII and/or financial information

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

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

3 37. The Notice included, *inter alia*, the claims that Defendant detected a network  
4 disruption on May 24, 2022 and launched an investigative process in which it discovered  
5 Representative Plaintiff’s and Class Members’ PHI/PII was affected.

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

10 39. Defendant had and continues to have obligations created by applicable federal and  
11 state and federal law as set forth herein, reasonable industry standards, common law, and its own  
12 assurances and representations to keep Representative Plaintiff’s and Class Members’ PHI/PII  
13 confidential and to protect such PHI/PII from unauthorized access.

14 40. Representative Plaintiff and Class Members were required to provide their PHI/PII  
15 and financial information to Defendant in order to obtain/retain employment with Defendant, and  
16 as part of Defendant’s business activities, Defendant created, collected, and stored Representative  
17 Plaintiff’s and Class Members’ data with the reasonable expectation and mutual understanding  
18 that Defendant would comply with its obligations to keep such information confidential and secure  
19 from unauthorized access.

20 41. Despite this, Representative Plaintiff and the Class Members remain, even today,  
21 in the dark regarding what particular data was stolen, the particular malware used, and what steps  
22 are being taken, if any, to secure their PHI/PII and financial information going forward.  
23 Representative Plaintiff and Class Members are, thus, left to speculate as to where their PHI/PII  
24 ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to  
25 further speculate as to the full impact of the Data Breach and how exactly Defendant intend to  
26 enhance its information security systems and monitoring capabilities so as to prevent further  
27 breaches.

28

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

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

7  
8 **Defendant Collected/Stored Class Members’ PHI/PII and Financial Information**

9           43. Defendant acquired, collected, and stored and assured reasonable security over  
10 Representative Plaintiff’s and Class Members’ PHI/PII and financial information.

11           44. As a condition of its relationships with Representative Plaintiff and Class Members,  
12 Defendant required that Representative Plaintiff and Class Members entrust Defendant with highly  
13 sensitive and confidential PHI/PII and financial information. Defendant, in turn, stored that  
14 information of Defendant’s system that was ultimately affected by the Data Breach.

15           45. By obtaining, collecting, and storing Representative Plaintiff’s and Class Members’  
16 PHI/PII and financial information, Defendant assumed legal and equitable duties and knew or  
17 should have known that it was thereafter responsible for protecting Representative Plaintiff’s and  
18 Class Members’ PHI/PII and financial information from unauthorized disclosure.

19           46. Representative Plaintiff and Class Members have taken reasonable steps to  
20 maintain the confidentiality of their PHI/PII and financial information. Representative Plaintiff  
21 and Class Members relied on Defendant to keep their PHI/PII and financial information  
22 confidential and securely maintained, to use this information for business and human resources  
23 purposes only, and to make only authorized disclosures of this information.

24           47. Defendant could have prevented the Data Breach by properly securing and  
25 encrypting and/or more securely encrypting its servers generally, as well as Representative  
26 Plaintiff’s and Class Members’ PHI/PII and financial information.

27           48. Defendant’s negligence in safeguarding Representative Plaintiff’s and Class  
28 Members’ PHI/PII and financial information is exacerbated by repeated warnings and alerts

1 directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks  
2 in recent years.

3 49. Due to the high-profile nature of recent data breaches, Defendant was and/or  
4 certainly should have been on notice and aware of such attacks occurring in the healthcare industry  
5 and, therefore, should have assumed and adequately performed the duty of preparing for such an  
6 imminent attack. This is especially true given that Defendant is a large, sophisticated operation  
7 with the resources to put adequate data security protocols in place.

8 50. Yet, despite the prevalence of public announcements of data breach and data  
9 security compromises, Defendant failed to take appropriate steps to protect Representative  
10 Plaintiff's and Class Members' PHI/PII from being compromised.

11  
12 **Defendant Had an Obligation to Protect the Stolen Information**

13 51. Defendant's failure to adequately secure Representative Plaintiff's and Class  
14 Members' sensitive data breaches duties it owes Representative Plaintiff and Class Members under  
15 statutory and common law. Moreover, Representative Plaintiff and Class Members surrendered  
16 their highly sensitive personal data to Defendant under the implied condition that Defendant would  
17 keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their  
18 data, independent of any statute.

19 52. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC  
20 Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting  
21 commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure  
22 to maintain reasonable and appropriate data security for consumers' sensitive personal information  
23 is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*,  
24 799 F.3d 236 (3d Cir. 2015).

25 53. In addition to its obligations under federal and state laws, Defendant owed a duty  
26 to Representative Plaintiff and Class Members to exercise reasonable care in obtaining, retaining,  
27 securing, safeguarding, deleting, and protecting the PHI/PII and financial information in  
28 Defendant's possession from being compromised, lost, stolen, accessed, and misused by

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

1 unauthorized persons. Defendant owed a duty to Representative Plaintiff and Class Members to  
2 provide reasonable security, including consistency with industry standards and requirements, and  
3 to ensure that its computer systems, networks, and protocols adequately protected the PHI/PII and  
4 financial information of Representative Plaintiff and Class Members.

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

8 55. Defendant owed a duty to Representative Plaintiff and Class Members to create and  
9 implement reasonable data security practices and procedures to protect the PHI/PII and financial  
10 information in its possession, including not sharing information with other/her/their entities who  
11 maintained sub-standard data security systems.

12 56. Defendant owed a duty to Representative Plaintiff and Class Members to  
13 implement processes that would immediately detect a breach on its data security systems in a  
14 timely manner.

15 57. Defendant owed a duty to Representative Plaintiff and Class Members to act upon  
16 data security warnings and alerts in a timely fashion.

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

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

23 60. Defendant owed a duty to Representative Plaintiff and Class Members to encrypt  
24 and/or more reliably encrypt Representative Plaintiff's and Class Members' PHI/PII and financial  
25 information and monitor user behavior and activity in order to identify possible threats.

26  
27  
28

1 **Value of the Relevant Sensitive Information**

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

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

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

19 64. The FTC defines identity theft as “a fraud committed or attempted using the  
 20 identifying information of another person without authority.” The FTC describes “identifying

21 <sup>3</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct.  
 22 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed July 28, 2021).

23 <sup>4</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.  
 24 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed November 5, 2021).

25 <sup>5</sup> *In the Dark*, VPNOverview, 2019, available at:  
<https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed January 21,  
 26 2022).

26 <sup>6</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133> (last  
 27 accessed January 21, 2022).

27 <sup>7</sup> <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed  
 28 January 21, 2022).

28 <sup>8</sup> <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches> (last accessed January 21, 2022).

1 information” as “any name or number that may be used, alone or in conjunction with any other  
 2 information, to identify a specific person,” including, among other things, “[n]ame, Social Security  
 3 number, date of birth, official State or government issued driver’s license or identification number,  
 4 alien registration number, government passport number, employer or taxpayer identification  
 5 number.”

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

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

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

25 [L]aw enforcement officials told us that in some cases, stolen data may be held for  
 26 up to a year or more before being used to commit identity theft. Further, once stolen  
 27 data have been sold or posted on the Web, fraudulent use of that information may  
 28 continue for years. As a result, studies that attempt to measure the harm resulting  
 from data breaches cannot necessarily rule out all future harm.<sup>9</sup>

<sup>9</sup> *Report to Congressional Requesters, GAO, at 29 (June 2007), available at:*

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

68. When cyber criminals access Social Security numbers—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Representative Plaintiff and Class Members.

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

70. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.<sup>13</sup>

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

---

<http://www.gao.gov/new.items/d07737.pdf> (last accessed January 21, 2022).  
<sup>10</sup> Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)  
<sup>11</sup> *Id.* at 17.  
<sup>12</sup> *Id.* at 28.  
<sup>13</sup> *Id.*



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

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

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

8           78. Defendant knew, or should have known, that its data systems and networks did not  
9 adequately safeguard Representative Plaintiff’s and Class Members’ PHI/PII and financial  
10 information.

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

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

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

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

25           83. Defendant also had independent duties under state and federal laws that required  
26 Defendant to reasonably safeguard Representative Plaintiff’s and Class Members’ PHI/PII and  
27 financial information and promptly notify them about the Data Breach. These “independent duties”  
28

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

1 are untethered to any contract between Defendant and Representative Plaintiff and/or the  
2 remaining Class Members.

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

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

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

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

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

1           87. The law further imposes an affirmative duty on Defendant to timely disclose the  
2 unauthorized access and theft of the PHI/PII and financial information to Representative Plaintiff  
3 and Class Members so that they could and/or still can take appropriate measures to mitigate  
4 damages, protect against adverse consequences and thwart future misuse of its PHI/PII and  
5 financial information.

6           88. Defendant breached its duty to notify Representative Plaintiff and Class Members  
7 of the unauthorized access by waiting months after learning of the Data Breach to notify  
8 Representative Plaintiff and Class Members and then by failing and continuing to fail to provide  
9 Representative Plaintiff and Class Members sufficient information regarding the breach. To date,  
10 Defendant have not provided sufficient information to Representative Plaintiff and Class Members  
11 regarding the extent of the unauthorized access and continues to breach its disclosure obligations  
12 to Representative Plaintiff and Class Members.

13           89. Further, through its failure to provide timely and clear notification of the Data  
14 Breach to Representative Plaintiff and Class Members, Defendant prevented Representative  
15 Plaintiff and Class Members from taking meaningful, proactive steps to secure its PHI/PII and  
16 financial information, and to access its medical records and histories.

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

24           91. Defendant’s wrongful actions, inactions, and omissions constituted (and continue  
25 to constitute) common law negligence.

26           92. The damages Representative Plaintiff and Class Members have suffered (as alleged  
27 above) and will suffer were and are the direct and proximate result of Defendant’s grossly  
28 negligent conduct.

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

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

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

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

3 102. Each of Defendant’s statutory violations of Section 5 of the FTC Act and other  
4 applicable statutes, rules, and regulations, constitute negligence *per se*.

5 103. Representative Plaintiff and the Class Members are within the category of persons  
6 the FTC Act were intended to protect.

7 104. The harm that occurred as a result of the Data Breach described herein is the type  
8 of harm the FTC Act was intended to guard against.

9 105. As a direct and proximate result of Defendant’s negligence *per se*, Plaintiff and  
10 Class Members have been damaged as described herein, continue to suffer injuries as detailed  
11 above, are subject to the continued risk of exposure of their PHI/PII in Defendant’s possession,  
12 and are entitled to damages in an amount to be proven at trial.

13  
14 **THIRD CLAIM FOR RELIEF**  
15 **Confidentiality of Medical Information Act**  
**(Cal. Civ. Code §56, et seq.)**  
16 **(On behalf of the California Subclass)**

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

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

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

25 4. As defined in the CMIA, California Civil Code §56.05(j), Defendant disclosed  
26 “medical information” to unauthorized persons without obtaining consent, in violation of  
27 §56.10(a). Defendant’s misconduct, including failure to adequately detect, protect, and prevent  
28 unauthorized disclosure, directly resulted in the unauthorized disclosure of Representative

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

1 Plaintiff's and California Subclass Members' PHI/PII and financial information to unauthorized  
2 persons.

3 5. Defendant's misconduct, including protecting and preserving the confidential  
4 integrity of its patients'/customers' PHI/PII and financial information, resulted in unauthorized  
5 disclosure of sensitive and confidential PII that belongs to Representative Plaintiff and California  
6 Subclass Members to unauthorized persons, breaching the confidentiality of that information,  
7 thereby violating California Civil Code §§ 56.06 and 56.101(a).

8 6. As a result of the Data Breach, unauthorized third parties viewed Representative  
9 Plaintiff's and Class Members' protected medical information.

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

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

21  
22 **FOURTH CLAIM FOR RELIEF**  
23 **Breach of Implied Contract**  
24 **(On behalf of the Nationwide Class and the California Subclass)**

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

27 10. Through its course of conduct, Defendant, Representative Plaintiff and Class  
28 Members entered into implied contracts for Defendant to implement data security adequate to

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

1 safeguard and protect the privacy of Representative Plaintiff’s and Class Members’ PHI/PII and  
2 financial information.

3 11. Defendant required Representative Plaintiff and Class Members to provide and  
4 entrust their PHI/PII and financial information as a condition of obtaining Defendant’s good.

5 12. Defendant solicited and invited Representative Plaintiff and Class Members to  
6 provide their PHI/PII and financial information as part of Defendant’s regular business practices.  
7 Representative Plaintiff and Class Members accepted Defendant’s offers and provided their  
8 PHI/PII and financial information to Defendant.

9 13. As a condition of their relationship with Defendant, Representative Plaintiff and  
10 Class Members provided and entrusted their PHI/PII and financial information to Defendant. In so  
11 doing, Representative Plaintiff and Class Members entered into implied contracts with Defendant  
12 by which Defendant agreed to safeguard and protect such non-public information, to keep such  
13 information secure and confidential, and to timely and accurately notify Representative Plaintiff  
14 and Class Members if its data had been breached and compromised or stolen.

15 14. A meeting of the minds occurred when Representative Plaintiff and Class Members  
16 agreed to, and did, provide their PHI/PII and financial information to Defendant, in exchange for,  
17 amongst other things, the protection of their PHI/PII and financial information.

18 15. Representative Plaintiff and Class Members fully performed their obligations under  
19 the implied contracts with Defendant.

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

24 17. As a direct and proximate result of Defendant’s above-described breach of implied  
25 contract, Representative Plaintiff and Class Members have suffered (and will continue to suffer)  
26 (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting  
27 in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting  
28 in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data;

1 (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other  
2 economic and non-economic harm.

3 **FIFTH CLAIM FOR RELIEF**  
4 **Breach of the Implied Covenant of Good Faith and Fair Dealing**  
5 **(On behalf of the Nationwide Class and the California Subclass)**

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

8 19. Every contract in this state has an implied covenant of good faith and fair dealing.  
9 This implied covenant is an independent duty and may be breached even when there is no  
10 breach of a contract's actual and/or express terms.

11 20. Representative Plaintiff and Class Members have complied with and performed all  
12 conditions of their contracts with Defendant.

13 21. Defendant breached the implied covenant of good faith and fair dealing by failing  
14 to maintain adequate computer systems and data security practices to safeguard PHI/PII and  
15 financial information, failing to timely and accurately disclose the Data Breach to Representative  
16 Plaintiff and Class Members and continued acceptance of PHI/PII and financial information and  
17 storage of other personal information after Defendant knew, or should have known, of the security  
18 vulnerabilities of the systems that were exploited in the Data Breach.

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

22 **SIXTH CLAIM FOR RELIEF**  
23 **Unfair Business Practices**  
24 **(Cal. Bus. & Prof. Code, §17200, et seq.)**  
25 **(On behalf of the California Subclass)**

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

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

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

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

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

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

7           27. The knowing conduct of Defendant, as alleged herein, constitutes an unlawful  
8 and/or fraudulent business practice, as set forth in California Business & Professions Code  
9 §§17200-17208. Specifically, Defendant conducted business activities while failing to comply  
10 with the legal mandates cited herein, including HIPAA. Such violations include, but are not  
11 necessarily limited to:

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

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

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

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

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

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

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

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

21

22 **SEVENTH CLAIM FOR RELIEF**  
23 **Unjust Enrichment**  
24 **(On behalf of the Nationwide Class and the California Subclass)**

25 34. Each and every allegation of the preceding paragraphs is incorporated in this cause  
26 of action with the same force and effect as though fully set forth therein.

27 35. By its wrongful acts and omissions described herein, Defendant has obtained a  
28 benefit by unduly taking advantage 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           36. Representative Plaintiff entrusted her PHI/PII and financial information to  
2 Defendant in the course of her employment with Defendant. This caused Representative Plaintiff  
3 to reasonably believe that Defendant would keep such PHI/PII and financial information secure.  
4 The remaining Class Members provided Defendant with their PHI/PII and financial information  
5 for similar purposes and—likewise—reasonably believed Defendant would keep their PHI/PII and  
6 financial information secure.

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

11           38. Defendant was also aware that, if the substandard condition of and vulnerabilities  
12 in its information systems were disclosed, it would negatively affect Representative Plaintiff’s and  
13 Class Members’ decisions to seek products/services therefrom.

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

21           40. Defendant was unjustly enriched at the expense of Representative Plaintiff and  
22 Class Members. Defendant received profits, benefits, and compensation, in part, at the expense of  
23 Representative Plaintiff and Class Members. By contrast, Representative Plaintiff and Class  
24 Members did not receive the benefit of their bargain because they paid for products that did not  
25 satisfy the purposes for which they bought/sought them.

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

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

5  
6 **RELIEF SOUGHT**

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

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

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

16 3. That the Court enjoin Defendant, ordering them to cease and desist from unlawful  
17 activities;

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

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

- 25 a. prohibiting Defendant from engaging in the wrongful and unlawful acts  
26 described herein;  
27 b. requiring Defendant to protect, including through encryption, all data  
28 collected through the course of business in accordance with all applicable  
regulations, industry standards, and federal, state, or local laws;

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

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

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

- c. requiring Defendant to delete and purge the PHI/PII 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' PHI/PII;
- e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;
- f. prohibiting Defendant from maintaining Representative Plaintiff's and Class Members' PHI/PII on a cloud-based database;
- g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- h. requiring Defendant to conduct regular database scanning and securing checks;
- i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling 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;
- l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

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

Complaint.

**JURY DEMAND**

Representative Plaintiff, individually and on behalf of the Plaintiff Classes and/or Subclasses, hereby demands a trial by jury for all issues triable by jury.

Dated: October 7, 2022

**COLE & VAN NOTE**

By: /s/ Cody A. Bolce.  
Cody A. Bolce, Esq.  
Attorneys for Representative Plaintiff  
and the Plaintiff Classes

**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