

1 Laura Grace Van Note, Esq. (S.B. #310160)  
Elizabeth Ruth Klos, Esq. (S.B. #346781)  
2 **COLE & VAN NOTE**  
555 12<sup>th</sup> Street, Suite 2100  
3 Oakland, California 94607  
Telephone: (510) 891-9800  
4 Facsimile: (510) 891-7030  
Email: lvn@colevannote.com  
5 Email: erk@colevannote.com  
Web: www.colevannote.com

6  
7 Kevin Laukaitis (*Pro hac vice* application forthcoming)  
**LAUKAITIS LAW LLC**  
954 Avenida Ponce De Leon  
8 Suite 205 - #10518  
San Juan, PR 00907  
9 Telephone: (215) 789-4462  
Email: klaukaitis@laukaitislaw.com

10  
11 Attorneys for Representative Plaintiff  
and the Plaintiff Class(es)

12  
13 **UNITED STATES DISTRICT COURT**  
14 **NORTHERN DISTRICT OF CALIFORNIA**

15  
16 BENJAMIN FISHER and BRITTANY  
HALLMAN, individually, and on behalf of  
17 all others similarly situated,

18 Plaintiffs,

19 v.

20 POSTMEDS, INC. d/b/a TRUEPILL

21 Defendant.

**Case No.**

**CLASS ACTION**

**COMPLAINT FOR DAMAGES**

**[JURY TRIAL DEMANDED]**

22  
23  
24 Plaintiffs Benjamin Fisher and Brittany Hallman (“Plaintiffs”) bring this class action  
25 against Defendant Postmeds, Inc. d/b/a TruePill (“Defendant”) for its failure to properly secure  
26 and safeguard Plaintiffs’ and Class Members’ personally identifiable information (“PII”) and  
27 protected health information (“PHI”) (collectively “PII/PHI”) stored within Defendant’s  
28 information network.

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

**INTRODUCTION**

1  
2  
3 1. Defendant is a healthcare services company and pharmacy.

4 2. Defendant acquired, collected, and stored Plaintiffs’ and Class Members’ PII/PHI.

5 3. At all relevant times, Defendant knew or should have known, that Plaintiffs and  
6 Class Members would use Defendant’s services to store and/or share sensitive data, including  
7 highly confidential PII/PHI.

8 4. On no later than August 30, 2023, upon information and belief, unauthorized third-  
9 party cybercriminals gained access to Plaintiffs’ and Class Members’ PII/PHI as hosted with  
10 Defendant, with the intent of engaging in the misuse of the PII/PHI, including marketing,  
11 disseminating, and selling Plaintiffs’ and Class Members’ PII/PHI.

12 5. The total number of individuals who have had their data exposed due to  
13 Defendant’s failure to implement appropriate security safeguards is unknown at this time but is  
14 estimated to be hundreds of thousands of individuals at a minimum, based on Defendant’s  
15 clientele.

16 6. Personally identifiable information (“PII”) generally incorporates information that  
17 can be used to distinguish or trace an individual’s identity, and is generally defined to include  
18 certain identifiers that do not on their face name an individual, but that is considered to be  
19 particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers,  
20 passport numbers, driver’s license numbers, financial account numbers).

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

26 8. The vulnerable and potentially exposed data at issue of Plaintiffs and the Class  
27 stored on Defendant’s information network, includes, without limitation: names and prescription  
28 information, including medication type, demographic information, and/or prescribing physician.

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 Plaintiffs and Class Members by intentionally,  
2 willfully, recklessly, or negligently failing to take and implement adequate and reasonable  
3 measures to ensure that Plaintiffs’ and Class Members’ PII/PHI was safeguarded, failing to take  
4 available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required  
5 and appropriate protocols, policies and procedures regarding the encryption of data, even for  
6 internal use.

7 10. As a result, the PII/PHI of Plaintiffs and Class Members was compromised through  
8 disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that  
9 seeks to profit off this disclosure by defrauding Plaintiffs and Class Members in the future.

10 11. Plaintiffs and Class Members have a continuing interest in ensuring that their  
11 information is and remains safe, and they are thus entitled to injunctive and other equitable relief.  
12

13 JURISDICTION AND VENUE

14 12. 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 class member is a citizen of a state different from Defendant.

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

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

25 15. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of  
26 the events that gave rise to Plaintiffs’ claims occurred within this District, and Defendant does  
27 business in this Judicial District.  
28

1 **DIVISIONAL ASSIGNMENT**

2 16. Pursuant to Civil L.R. 3-2(c), this Action should be assigned to either the San  
3 Francisco or the Oakland Division, as Defendant’s principal place of business is located in  
4 Alameda County, California and the events giving rise to Plaintiffs’ claims occurred in Alameda  
5 County, California.

6  
7 **THE PARTIES**

8 ***Plaintiff Benjamin Fisher***

9 17. Plaintiff Fisher is an adult individual and, at all relevant times herein, a resident and  
10 citizen of Louisiana. Plaintiff Fisher is a victim of the Data Breach.

11 18. Plaintiff Fisher was a direct client or a client of a business serviced by Defendant,  
12 and his information was stored with Defendant as a result of his dealings with Defendant.

13 19. As required in order to obtain services from Defendant, Plaintiff Fisher provided  
14 Defendant with highly sensitive personal information, who then possessed and controlled it.

15 20. As a result, Plaintiff Fisher’s information was among the data accessed by an  
16 unauthorized third-party in the Data Breach.

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

19 22. Plaintiff Fisher received a notice from Defendant, dated October 31, 2023, stating  
20 that his PII/PHI was involved in the Data Breach (the “Notice”).

21 23. As a result, Plaintiff Fisher was injured in the form of lost time dealing with the  
22 consequences of the Data Breach, which included and continues to include: time spent verifying  
23 the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity  
24 theft insurance options; time spent self-monitoring his accounts with heightened scrutiny and time  
25 spent seeking legal counsel regarding his options for remedying and/or mitigating the effects of  
26 the Data Breach.

27 24. Plaintiff Fisher was also injured by the material risk to future harm he suffers based  
28 on Defendant’s breach; this risk is imminent and substantial because Plaintiff Fisher’s data has

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

1 | been exposed in the breach, the data involved, including healthcare information, is highly sensitive  
 2 | and presents a high risk of identity theft or fraud; and it is likely, given Defendant’s clientele, that  
 3 | some of the Class’s information that has been exposed has already been misused.

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

7 | 26. Plaintiff Fisher, as a result of the Data Breach, has increased anxiety for his loss of  
 8 | privacy and anxiety over the impact of cybercriminals accessing, using, and selling his PII/PHI.

9 | 27. Plaintiff Fisher has suffered imminent and impending injury arising from the  
 10 | substantially increased risk of fraud, identity theft, and misuse resulting from his PII/PHI, in  
 11 | combination with his name, being placed in the hands of unauthorized third parties/criminals.

12 | 28. Plaintiff Fisher has a continuing interest in ensuring that his PII/PHI, which, upon  
 13 | information and belief, remains backed up in Defendant’s possession, is protected and safeguarded  
 14 | from future breaches.

15 | ***Plaintiff Brittany Hallman***

16 | 29. Plaintiff Hallman is an adult individual and, at all relevant times herein, a resident  
 17 | and citizen of South Carolina. Plaintiff Hallman is a victim of the Data Breach.

18 | 30. Plaintiff Hallman was a direct client or a client of a business serviced by Defendant,  
 19 | and her information was stored with Defendant as a result of her dealings with Defendant.

20 | 31. As required in order to obtain services from Defendant, Plaintiff Hallman provided  
 21 | Defendant with highly sensitive personal information, who then possessed and controlled it.

22 | 32. As a result, Plaintiff Hallman’s information was among the data accessed by an  
 23 | unauthorized third-party in the Data Breach.

24 | 33. At all times herein relevant, Plaintiff Hallman is and was a member of each of the  
 25 | Classes.

26 | 34. Plaintiff Hallman received a notice from Defendant, dated October 31, 2023, stating  
 27 | that her PII/PHI was involved in the Data Breach (the “Notice”).  
 28 |

1           35. As a result, Plaintiff Hallman was injured in the form of lost time dealing with the  
2 consequences of the Data Breach, which included and continues to include: time spent verifying  
3 the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity  
4 theft insurance options; time spent self-monitoring her accounts with heightened scrutiny and time  
5 spent seeking legal counsel regarding his options for remedying and/or mitigating the effects of  
6 the Data Breach.

7           36. Plaintiff Hallman was also injured by the material risk to future harm she suffers  
8 based on Defendant's breach; this risk is imminent and substantial because Plaintiff Hallman's  
9 data has been exposed in the breach, the data involved, including healthcare information, is highly  
10 sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's  
11 clientele, that some of the Class's information that has been exposed has already been misused.

12           37. Plaintiff Hallman suffered actual injury in the form of damages to and diminution  
13 in the value of her PII/PHI—a condition of intangible property that they entrusted to Defendant,  
14 which was compromised in and as a result of the Data Breach.

15           38. Plaintiff Hallman, as a result of the Data Breach, has increased anxiety for her loss  
16 of privacy and anxiety over the impact of cybercriminals accessing, using, and selling his PII/PHI.

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

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

23           ***Defendant Postmeds, Inc. d/b/a TruePill***

24           41. Defendant Postmeds, Inc., d/b/a TruePill, is a Delaware corporation with its  
25 principal place of business located at 3121 Diablo Avenue, Hayward, CA 94545.

26           42. The true names and capacities of persons or entities, whether individual, corporate,  
27 associate, or otherwise, who may be responsible for some of the claims alleged here are currently  
28 unknown to Plaintiffs.

1 43. Plaintiffs will seek leave of court to amend this Complaint to reflect the true names  
2 and capacities of the responsible parties when their identities become known.  
3

4 **CLASS ACTION ALLEGATIONS**

5 44. Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and  
6 (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and the following Class:

7 All individuals within the United States of America whose PII/PHI was exposed to  
8 unauthorized third-parties as a result of the data incident discovered by Defendant on August 31,  
9 2023.

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

17 46. Plaintiffs reserve the right to amend the above definitions or to propose subclasses  
18 in subsequent pleadings and motions for class certification.

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

22 48. Numerosity: A class action is the only available method for the fair and efficient  
23 adjudication of this controversy, as the members of the Class are so numerous that joinder of all  
24 members is impractical, if not impossible.

25 49. Commonality: Plaintiffs and the Class Members share a community of interests in  
26 that there are numerous common questions and issues of fact and law which predominate over any  
27 questions and issues solely affecting individual members, including, but not necessarily limited to:  
28

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 a. Whether Defendant had a legal duty to Plaintiffs and the Class to exercise
- 2 due care in collecting, storing, using, and/or safeguarding their PII/PHI;
- 3 b. Whether Defendant knew or should have known of the susceptibility of its
- 4 data security systems to a data breach;
- 5 c. Whether Defendant’s security procedures and practices to protect its
- 6 systems were reasonable in light of the measures recommended by data
- 7 security experts;
- 8 d. Whether Defendant’s failure to implement adequate data security measures
- 9 allowed the Data Breach to occur;
- 10 e. Whether Defendant failed to comply with its own policies and applicable
- 11 laws, regulations, and industry standards relating to data security;
- 12 f. Whether Defendant adequately, promptly, and accurately informed
- 13 Plaintiffs and Class Members that their PII/PHI had been compromised;
- 14 g. How and when Defendant actually learned of the Data Breach;
- 15 h. Whether Defendant’s conduct, including its failure to act, resulted in or was
- 16 the proximate cause of the breach of its systems, resulting in the loss of the
- 17 PII/PHI of Plaintiffs and Class Members;
- 18 i. Whether Defendant adequately addressed and fixed the vulnerabilities
- 19 which permitted the Data Breach to occur;
- 20 j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by
- 21 failing to safeguard the PII/PHI of Plaintiffs and Class Members;
- 22 k. Whether Plaintiffs and Class Members are entitled to actual and/or statutory
- 23 damages and/or whether injunctive, corrective and/or declaratory relief
- 24 and/or accounting is/are appropriate as a result of Defendant’s wrongful
- 25 conduct; and
- 26 l. Whether Plaintiffs and Class Members are entitled to restitution as a result
- 27 of Defendant’s wrongful conduct.
- 28



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

1           50.    Typicality: Plaintiffs’ claims are typical of the claims of the Class. Plaintiffs and all  
2 members of the Class sustained damages arising out of and caused by Defendant’s common course  
3 of conduct in violation of law, as alleged herein.

4           51.    Adequacy of Representation: Plaintiffs in this class action are adequate  
5 representatives of the Class in that the Plaintiffs have the same interest in the litigation of this case  
6 as the Class Members, are committed to the vigorous prosecution of this case and have retained  
7 competent counsel who are experienced in conducting litigation of this nature.

8           52.    Plaintiffs are not subject to any individual defenses unique from those conceivably  
9 applicable to other Class Members or the class in its entirety. Plaintiffs anticipate no management  
10 difficulties in this litigation.

11           53.    Superiority of Class Action: Since the damages suffered by individual Class  
12 Members, while not inconsequential, may be relatively small, the expense and burden of individual  
13 litigation by each member make or may make it impractical for members of the Class to seek  
14 redress individually for the wrongful conduct alleged herein. Should separate actions be brought  
15 or be required to be brought, by each individual member of the Class, the resulting multiplicity of  
16 lawsuits would cause undue hardship and expense for the Court and the litigants.

17           54.    The prosecution of separate actions would also create a risk of inconsistent rulings,  
18 which might be dispositive of the interests of the Class Members who are not parties to the  
19 adjudications and/or may substantially impede their ability to protect their interests adequately.

20           55.    This class action is also appropriate for certification because Defendant has acted  
21 or refused to act on grounds generally applicable to Class Members, thereby requiring the Court’s  
22 imposition of uniform relief to ensure compatible standards of conduct toward the Class Members  
23 and making final injunctive relief appropriate with respect to the Class in its entirety.

24           56.    Defendant’s policies and practices challenged herein apply to and affect Class  
25 Members uniformly and Plaintiffs’ challenge of these policies and practices hinges on Defendant’s  
26 conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiffs.

27  
28

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

4 58. 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 **Defendant's Failed Response to the Breach**

11 59. Not until after months it claims to have discovered the Data Breach did Defendant  
12 begin sending the Notice to persons whose PII/PHI Defendant confirmed was potentially  
13 compromised as a result of the Data Breach.

14 60. The Notice included, inter alia, basic details of the Data Breach, Defendant's  
15 recommended next steps, and Defendant's claims that it had learned of the Data Breach on August  
16 31, 2023, and completed a review thereafter.

17 61. Upon information and belief, the unauthorized third-party cybercriminals gained  
18 access to Plaintiffs' and Class Members' PII/PHI with the intent of engaging in the misuse of the  
19 PII/PHI, including marketing and selling Plaintiffs' and Class Members' PII/PHI.

20 62. Defendant had and continues to have obligations created by applicable federal and  
21 state law as set forth herein, reasonable industry standards, common law, and its own assurances  
22 and representations to keep Plaintiffs' and Class Members' PII/PHI confidential and to protect  
23 such PII/PHI from unauthorized access.

24 63. Plaintiffs and Class Members were required to provide their PII/PHI to Defendant  
25 as a part of using their services, and in doing so Defendant created the reasonable expectation and  
26 mutual understanding with Plaintiffs and Class Members that Defendant would comply with its  
27 obligations to keep such information confidential and secure 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

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

1           64. Despite this, Plaintiffs and the Class Members remain, even today, in the dark  
2 regarding what particular data was stolen, the particular malware used, and what steps are being  
3 taken, if any, to secure their PII/PHI going forward.

4           65. Plaintiffs and Class Members are, thus, left to speculate as to where their PII/PHI  
5 ended up, who has used it, and for what potentially nefarious purposes, and are left to further  
6 speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance  
7 its information security systems and monitoring capabilities to prevent further breaches.

8           66. Unauthorized individuals can now easily access the PII/PHI of Plaintiffs and Class  
9 Members.

10 **Defendant Collected/Stored Class Members' PII/PHI**

11           67. Defendant acquired, collected, and stored and assured reasonable security over  
12 Plaintiffs' and Class Members' PII/PHI.

13           68. As a condition of its relationships with Plaintiffs and Class Members, Defendant  
14 required that Plaintiffs and Class Members entrust Defendant with highly sensitive and  
15 confidential PII/PHI.

16           69. Defendant, in turn, stored that information in the part of Defendant's system that  
17 was ultimately affected by the Data Breach.

18           70. By obtaining, collecting, and storing Plaintiffs' and Class Members' PII/PHI,  
19 Defendant assumed legal and equitable duties and knew or should have known that they were  
20 thereafter responsible for protecting Plaintiffs' and Class Members' PII/PHI from unauthorized  
21 disclosure.

22           71. Plaintiffs and Class Members have taken reasonable steps to maintain the  
23 confidentiality of their PII/PHI.

24           72. Plaintiffs and Class Members relied on Defendant to keep their PII/PHI confidential  
25 and securely maintained, to use this information for business and healthcare purposes only, and to  
26 make only authorized disclosures of this information.

27  
28

1 73. Defendant could have prevented the Data Breach, which began no later than  
 2 September 1, 2023, by adequately securing and encrypting and/or more securely encrypting its  
 3 servers generally, as well as Plaintiffs' and Class Members' PII/PHI.

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

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

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

11 76. Defendant's failure to adequately secure Plaintiffs' and Class Members' sensitive  
 12 data breaches duties it owes Plaintiffs and Class Members under statutory and common law. Under  
 13 HIPAA, health insurance providers have an affirmative duty to keep patients' Protected Health  
 14 Information private. As a covered entity, Defendant has a statutory duty under HIPAA and other  
 15 federal and state statutes to safeguard Plaintiffs' and Class Members' data.

16 77. Moreover, Plaintiffs and Class Members surrendered their highly sensitive personal  
 17 data to Defendant under the implied condition that Defendant would keep it private and secure.  
 18 Accordingly, Defendant also has an implied duty to safeguard their data, independent of any  
 19 statute.

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

25 79. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health  
 26 Information establishes national standards for protecting health information.

27  
 28

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

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

4           81.    HIPAA requires Defendant to “comply with the applicable standards,  
5 implementation specifications, and requirements” of HIPAA “with respect to electronically  
6 protected health information.” 45 C.F.R. § 164.302.

7           82.    “Electronic protected health information” is “individually identifiable health  
8 information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45  
9 C.F.R. § 160.103.

10          83.    HIPAA’s Security Rule requires Defendant to do the following:

- 11           a.    Ensure the confidentiality, integrity, and availability of all electronically  
12 protected health information the covered entity or business associate  
13 creates, receives, maintains, or transmits;
- 14           b.    Protect against any reasonably anticipated threats or hazards to the security  
15 or integrity of such information;
- 16           c.    Protect against any reasonably anticipated uses or disclosures of such  
17 information that are not permitted; and
- 18           d.    Ensure compliance by its workforce.

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

25          85.    Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414,  
26 requires Defendant to provide notice of the Data Breach to each affected individual “without  
27 unreasonable delay and in no case later than 60 days following the discovery of the breach.”  
28

1 86. Defendant was prohibited by the Federal Trade Commission Act (the “FTC Act”)  
 2 (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting  
 3 commerce.”<sup>1</sup>

4 87. In addition to its obligations under federal and state laws, Defendant owed a duty  
 5 to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing,  
 6 safeguarding, deleting, and protecting the PII/PHI in Defendant’s possession from being  
 7 compromised, lost, stolen, accessed, and misused by unauthorized persons.

8 88. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable  
 9 security, including consistency with industry standards and requirements, and to ensure that its  
 10 computer systems, networks, and protocols adequately protected the PII/PHI of Plaintiffs and  
 11 Class Members.

12 89. Defendant owed a duty to Plaintiffs and Class Members to design, maintain, and  
 13 test its computer systems, servers, and networks to ensure that the PII/PHI was adequately secured  
 14 and protected.

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

18 91. Defendant owed a duty to Plaintiffs and Class Members to implement processes  
 19 that would immediately detect a breach in its data security systems in a timely manner.

20 92. Defendant owed a duty to Plaintiffs and Class Members to act upon data security  
 21 warnings and alerts in a timely fashion.

22 93. Defendant owed a duty to Plaintiffs and Class Members to disclose if its computer  
 23 systems and data security practices were inadequate to safeguard individuals’ PII/PHI from theft  
 24 because such an inadequacy would be a material fact in the decision to entrust this PII/PHI to  
 25 Defendant.

26  
 27 <sup>1</sup> The Federal Trade Commission (the “FTC”) has concluded that a company’s failure to  
 28 maintain reasonable and appropriate data security for consumers’ sensitive personal information is  
 an “unfair practice” in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*,  
 799 F.3d 236 (3d Cir. 2015).

1 94. Defendant owed a duty of care to Plaintiffs and Class Members because they were  
2 foreseeable and probable victims of any inadequate data security practices.

3 95. Defendant owed a duty to Plaintiffs and Class Members to encrypt and/or more  
4 reliably encrypt Plaintiffs' and Class Members' PII/PHI and monitor user behavior and activity in  
5 order to identify possible threats.

6 **Value of the Relevant Sensitive Information**

7 96. PII/PHI are valuable commodities for which a "cyber black market" exists in which  
8 criminals openly post stolen payment card numbers, Social Security numbers, and other personal  
9 information on several underground internet websites.

10 97. Numerous sources cite dark web pricing for stolen identity credentials; for example,  
11 personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price  
12 range of \$50 to \$200<sup>2</sup>; Experian reports that a stolen credit or debit card number can sell for \$5 to  
13 \$110 on the dark web<sup>3</sup>; and other sources report that criminals can also purchase access to entire  
14 company data breaches from \$999 to \$4,995.<sup>4</sup>

15 98. Identity thieves can use PII/PHI, such as that of Plaintiffs and Class Members,  
16 which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims—for  
17 instance, identity thieves may commit various types of government fraud such as immigration  
18 fraud, obtaining a driver's license or identification card in the victim's name but with another's  
19 picture, using the victim's information to obtain government benefits, or filing a fraudulent tax  
20 return using the victim's information to obtain a fraudulent refund.

21 99. There may be a time lag between when harm occurs versus when it is discovered,  
22 and also between when PII/PHI is stolen and when it is used: according to the U.S. Government  
23 Accountability Office ("GAO"), which conducted a study regarding data breaches:

24  
25 <sup>2</sup> *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed November 7, 2023).

26 <sup>3</sup> *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed November 7, 2023).

27 <sup>4</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed November 7, 2023).  
28

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

1 [L]aw enforcement officials told us that in some cases, stolen data might be held  
2 for up to a year or more before being used to commit identity theft. Further, once  
3 stolen data have been sold or posted on the Web, fraudulent use of that information  
may 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>5</sup>

4 100. Here, Defendant knew of the importance of safeguarding PII/PHI and of the  
5 foreseeable consequences that would occur if Plaintiffs' and Class Members' PII/PHI were stolen,  
6 including the significant costs that would be placed on Plaintiffs and Class Members as a result of  
7 a breach of this magnitude.

8 101. As detailed above, Defendant is a large, sophisticated organization with the  
9 resources to deploy robust cybersecurity protocols. It knew, or should have known, that the  
10 development and use of such protocols were necessary to fulfill its statutory and common law  
11 duties to Plaintiffs and Class Members. Therefore, its failure to do so is intentional, willful,  
12 reckless and/or grossly negligent.

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

21  
22 **CLAIMS FOR RELIEF**

23 **COUNT ONE**

24 **Negligence  
(On behalf of the Class)**

25 103. Plaintiffs reallege and reincorporate every allegation set forth in the preceding  
26 paragraphs as though fully set forth herein.

27  
28 <sup>5</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:  
<http://www.gao.gov/new.items/d07737.pdf> (last accessed November 7, 2023).



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

1           104. At all times herein relevant, Defendant owed Plaintiffs and Class Members a duty  
2 of care, inter alia, to act with reasonable care to secure and safeguard their PII/PHI and to use  
3 commercially reasonable methods to do so. Defendant took on this obligation upon accepting and  
4 storing the PII/PHI of Plaintiffs and Class Members in its computer systems and on its networks.

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

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

19           107. Defendant knew, or should have known, of the risks inherent in collecting and  
20 storing PII/PHI, the vulnerabilities of its data security systems, and the importance of adequate  
21 security.

22           108. Defendant knew about numerous, well-publicized data breaches.

23           109. Defendant knew, or should have known, that its data systems and networks did not  
24 adequately safeguard Plaintiffs' and Class Members' PII/PHI.

25           110. Only Defendant was in the position to ensure that its systems and protocols were  
26 sufficient to protect the PII/PHI that Plaintiffs and Class Members had entrusted to it.  
27  
28

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

1 111. Defendant breached its duties to Plaintiffs and Class Members by failing to provide  
2 fair, reasonable, or adequate computer systems and data security practices to safeguard their  
3 PII/PHI.

4 112. Because Defendant knew that a breach of its systems could damage thousands of  
5 individuals, including Plaintiffs and Class Members, Defendant had a duty to adequately protect  
6 its data systems and the PII/PHI contained therein.

7 113. Plaintiffs' and Class Members' willingness to entrust Defendant with their PII/PHI  
8 was predicated on the understanding that Defendant would take adequate security precautions.

9 114. Moreover, only Defendant had the ability to protect its systems and the PII/PHI is  
10 stored on them from attack. Thus, Defendant had a special relationship with Plaintiffs and Class  
11 Members.

12 115. Defendant also had independent duties under state and federal laws that required  
13 Defendant to reasonably safeguard Plaintiffs' and Class Members' PII/PHI and promptly notify  
14 them about the Data Breach. These "independent duties" are untethered to any contract between  
15 Defendant, Plaintiffs, and/or the remaining Class Members.

16 116. Defendant breached its general duty of care to Plaintiffs and Class Members in, but  
17 not necessarily limited to, the following ways:

- 18 a. by failing to provide fair, reasonable, or adequate computer systems and  
19 data security practices to safeguard the PII/PHI of Plaintiffs and Class  
20 Members;
- 21 b. by failing to timely and accurately disclose that Plaintiffs' and Class  
22 Members' PII/PHI had been improperly acquired or accessed;
- 23 c. by failing to adequately protect and safeguard the PII/PHI by knowingly  
24 disregarding standard information security principles, despite obvious risks,  
25 and by allowing unmonitored and unrestricted access to unsecured PII/PHI;
- 26 d. by failing to provide adequate supervision and oversight of the PII/PHI with  
27 which it was and is entrusted, in spite of the known risk and foreseeable  
28 likelihood of breach and misuse, which permitted an unknown third party

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

- 1 to gather PII/PHI of Plaintiffs and Class Members, misuse the PII/PHI and
- 2 intentionally disclose it to others without consent;
- 3 e. by failing to adequately train its employees not to store PII/PHI longer than
- 4 absolutely necessary;
- 5 f. by failing to consistently enforce security policies aimed at protecting
- 6 Plaintiffs' and the Class Members' PII/PHI;
- 7 g. by failing to implement processes to detect data breaches, security incidents,
- 8 or intrusions quickly; and
- 9 h. by failing to encrypt Plaintiffs' and Class Members' PII/PHI and monitor
- 10 user behavior and activity in order to identify possible threats.

11 117. Defendant's willful failure to abide by these duties was wrongful, reckless, and

12 grossly negligent in light of the foreseeable risks and known threats.

13 118. As a proximate and foreseeable result of Defendant's grossly negligent conduct,

14 Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms

15 and damages.

16 119. To date, Defendant has not provided sufficient information to Plaintiffs and Class

17 Members regarding the extent of the unauthorized access and continues to breach its disclosure

18 obligations to Plaintiffs and Class Members.

19 120. Further, through its failure to provide clear notification of the Data Breach to

20 Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking

21 meaningful, proactive steps to secure their PII/PHI.

22 121. There is a close causal connection between Defendant's failure to implement

23 security measures to protect the PII/PHI of Plaintiffs and Class Members and the harm suffered,

24 or risk of imminent harm suffered by Plaintiffs and Class Members.

25 122. Plaintiffs' and Class Members' PII/PHI was accessed as the proximate result of

26 Defendant's failure to exercise reasonable care in safeguarding such PII/PHI by adopting,

27 implementing, and maintaining appropriate security measures.

28

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

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

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

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

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

24            127. Additionally, as a direct and proximate result of Defendant’s negligence, Plaintiffs  
25 and Class Members have suffered and will suffer the continued risks of exposure of their PII/PHI,  
26 which remain in Defendant’s possession and are subject to further unauthorized disclosures so  
27 long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI in  
28 its continued possession.

**COUNT TWO**  
**Breach of Implied Contract**  
**(On behalf of the Class)**

1  
2  
3 128. Plaintiffs reallege and reincorporate every allegation set forth in the preceding  
4 paragraphs as though fully set forth herein.

5 129. Through its course of conduct Plaintiffs and Class Members entered into implied  
6 contracts for Defendant to implement data security adequate to safeguard and protect the privacy  
7 of Plaintiffs' and Class Members' PII/PHI.

8 130. Defendant required Plaintiffs and Class Members to provide and entrust their  
9 PII/PHI as a condition of obtaining Defendant's services.

10 131. Defendant solicited and invited Plaintiffs and Class Members to provide their  
11 PII/PHI as part of Defendant's regular business practices.

12 132. Plaintiffs and Class Members accepted Defendant's offers and provided their  
13 PII/PHI to Defendant.

14 133. As a condition of being consumers of Defendant, Plaintiffs and Class Members  
15 provided and entrusted their PII/PHI to Defendant.

16 134. In so doing, Plaintiffs and Class Members entered into implied contracts with  
17 Defendant by which Defendant agreed to safeguard and protect such non-public information, to  
18 keep such information secure and confidential, and to timely and accurately notify Plaintiffs and  
19 Class Members if their data had been breached and compromised or stolen.

20 135. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and  
21 did, provide their PII/PHI to Defendant, in exchange for, amongst other things, the protection of  
22 their PII/PHI.

23 136. Plaintiffs and Class Members fully performed their obligations under the implied  
24 contracts with Defendant.

25 137. Defendant breached its implied contracts with Plaintiffs and Class Members by  
26 failing to safeguard and protect their PII/PHI and by failing to provide accurate notice to them that  
27 their PII/PHI was compromised as a result of the Data Breach.  
28

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

1 138. As a direct and proximate result of Defendant’s above-described breach of implied  
2 contract, Plaintiffs and Class Members have suffered (and will continue to suffer) (a) ongoing,  
3 imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary  
4 loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary  
5 loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal  
6 sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-  
7 economic harm.

8  
9 **COUNT THREE**  
10 **Breach of the Implied Covenant of Good Faith and Fair Dealing**  
11 **(On behalf of the Class)**

12 139. Plaintiffs reallege and reincorporate every allegation set forth in the preceding  
13 paragraphs as though fully set forth herein.

14 140. Every contract in this State has an implied covenant of good faith and fair dealing,  
15 which is an independent duty and may be breached even when there is no breach of a contract’s  
16 actual and/or express terms.

17 141. Plaintiffs and Class Members have complied with and performed all conditions of  
18 their contracts with Defendant.

19 142. Defendant breached the implied covenant of good faith and fair dealing by failing  
20 to maintain adequate computer systems and data security practices to safeguard PII/PHI, failing to  
21 timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued  
22 acceptance of PII/PHI and storage of other personal information after Defendant knew, or should  
23 have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

24 143. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and  
25 Class Members the full benefit of their bargains as originally intended by the parties, thereby  
26 causing them injury in an amount to be determined at trial.  
27  
28

**COUNT FOUR**  
**Unjust Enrichment**  
**(On behalf of the Class)**

1  
2  
3 144. Plaintiffs reallege and reincorporate every allegation set forth in the preceding  
4 paragraphs as though fully set forth herein.

5 145. By its wrongful acts and omissions described herein, Defendant has obtained a  
6 benefit by unduly taking advantage of Plaintiffs and Class Members.

7 146. Defendant, prior to and at the time Plaintiffs and Class Members entrusted their  
8 PII/PHI to Defendant for the purpose of obtaining Defendant's services, caused Plaintiffs and  
9 Class Members to reasonably believe that Defendant would keep such PII/PHI secure.

10 147. Defendant was aware, or should have been aware, that reasonable patients and  
11 consumers would have wanted their PII/PHI kept secure and would not have contracted with  
12 Defendant, directly or indirectly, had they known that Defendant's information systems were sub-  
13 standard for that purpose.

14 148. Defendant was also aware that, if the substandard condition of and vulnerabilities  
15 in its information systems were disclosed, it would negatively affect Plaintiffs' and Class  
16 Members' decisions to seek services therefrom.

17 149. Defendant failed to disclose facts pertaining to its substandard information systems,  
18 defects, and vulnerabilities therein before Plaintiffs and Class Members made their decisions to  
19 make purchases, engage in commerce therewith, and seek services or information.

20 150. Instead, Defendant suppressed and concealed such information. By concealing and  
21 suppressing that information, Defendant denied Plaintiffs and Class Members the ability to make  
22 a rational and informed purchasing decision and took undue advantage of Plaintiffs and Class  
23 Members.

24 151. Defendant was unjustly enriched at the expense of Plaintiffs and Class Members,  
25 as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiffs and  
26 Class Members; however, Plaintiffs and Class Members did not receive the benefit of their bargain  
27 because they paid for services that did not satisfy the purposes for which they bought/sought them.  
28

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

1 152. Since Defendant's profits, benefits, and other compensation were obtained  
2 improperly, Defendant is not legally or equitably entitled to retain any of the benefits,  
3 compensation or profits it realized from these transactions.

4 153. Plaintiffs and Class Members seek an Order of this Court requiring Defendant to  
5 refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by  
6 Defendant from its wrongful conduct and/or the establishment of a constructive trust from which  
7 Plaintiffs and Class Members may seek restitution.

8  
9 **PRAYER FOR RELIEF**

10 WHEREFORE, Plaintiffs, on behalf of themselves and each member of the proposed Class,  
11 respectfully request that the Court enter judgment in their favor and for the following specific relief  
12 against Defendant as follows:

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

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

18 3. That the Court enjoin Defendant, ordering them to cease from unlawful activities;

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

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

26 a. prohibiting Defendant from engaging in the wrongful and unlawful acts  
27 described herein;

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           b.     requiring Defendant to protect, including through encryption, all data
- 2                     collected through the course of business in accordance with all applicable
- 3                     regulations, industry standards, and federal, state, or local laws;
- 4           c.     requiring Defendant to delete and purge the PII/PHI of Plaintiffs and Class
- 5                     Members unless Defendant can provide to the Court reasonable justification
- 6                     for the retention and use of such information when weighed against the
- 7                     privacy interests of Plaintiffs and Class Members;
- 8           d.     requiring Defendant to implement and maintain a comprehensive
- 9                     Information Security Program designed to protect the confidentiality and
- 10                    integrity of Plaintiffs’ and Class Members’ PII/PHI;
- 11           e.     requiring Defendant to engage independent third-party security auditors and
- 12                     internal personnel to run automated security monitoring, simulated attacks,
- 13                     penetration tests, and audits on Defendant’s systems periodically;
- 14           f.     prohibiting Defendant from maintaining Plaintiffs’ and Class Members’
- 15                     PII/PHI on a cloud-based database;
- 16           g.     requiring Defendant to segment data by creating firewalls and access
- 17                     controls so that, if one area of Defendant’s network is compromised,
- 18                     hackers cannot gain access to other portions of Defendant’s systems;
- 19           h.     requiring Defendant to conduct regular database scanning and securing
- 20                     checks;
- 21           i.     requiring Defendant to establish an information security training program
- 22                     that includes at least annual information security training for all employees,
- 23                     with additional training to be provided as appropriate based upon the
- 24                     employees’ respective responsibilities with handling PII/PHI, as well as
- 25                     protecting the PII/PHI of Plaintiffs and Class Members;
- 26           j.     requiring Defendant to implement a system of tests to assess its respective
- 27                     employees’ knowledge of the education programs discussed in the
- 28                     preceding subparagraphs, as well as randomly and periodically testing

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

- 1 employees' compliance with Defendant's policies, programs, and systems
- 2 for protecting personal identifying information;
- 3 k. requiring Defendant to implement, maintain, review, and revise as
- 4 necessary a threat management program to monitor Defendant's networks
- 5 for internal and external threats appropriately, and assess whether
- 6 monitoring tools are properly configured, tested, and updated; and
- 7 l. requiring Defendant to meaningfully educate all Class Members about the
- 8 threats they face due to the loss of their confidential personal identifying
- 9 information to third parties, as well as the steps affected individuals must
- 10 take to protect themselves.
- 11 6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;
- 12 7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law;
- 13 and
- 14 8. For all other Orders, findings, and determinations identified and sought in this
- 15 Complaint.

**JURY DEMAND**

18 Plaintiffs, individually and on behalf of the Class, hereby demand a trial by jury for all  
19 issues triable by jury.

21 Dated: November 7, 2023

22

23 By: /s/ Elizabeth Ruth Klos  
 24 Laura Van Note, Esq. (C.A. S.B. #310160)  
 Elizabeth Ruth Klos, Esq. (C.A. S.B. #346781)  
**COLE & VAN NOTE**  
 25 555 12<sup>th</sup> Street, Suite 2100  
 Oakland, California 94607  
 Telephone: (510) 891-9800  
 26 Facsimile: (510) 891-7030  
 27 Email: lvn@colevannote.com

28

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

Kevin Laukaitis, Esq\*  
**LAUKAITIS LAW LLC**  
954 Avenida Ponce De Leon  
Suite 205 - #10518  
San Juan, PR 00907  
Telephone: (215) 789-4462  
Email: klaukaitis@laukaitislaw.com

*\*Pro hac vice forthcoming*

Attorneys for Representative Plaintiff and the  
Plaintiff Class