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

Attorneys for Representative Plaintiff and the Plaintiff Class

IN THE SUPERIOR COURT OF THE STATE OF CALIFORNIA

IN AND FOR THE COUNTY OF ALAMEDA

JOHN LAIRD, individually, and on behalf of all others similarly situated,

Plaintiff,

vs.

HELLO HOUSING and DOES 1 through 100, inclusive,

Defendants.

Case No. 22CV011872

CLASS ACTION

COMPLAINT FOR DAMAGES, INJUNCTIVE AND EQUITABLE RELIEF FOR:

1. **NEGLIGENCE;**
2. **CONFIDENTIALITY OF MEDICAL INFORMATION ACT (CAL. CIV. CODE §56);**
3. **BREACH OF IMPLIED CONTRACT;**
4. **UNFAIR BUSINESS PRACTICES;**

[JURY TRIAL DEMANDED]

Representative Plaintiff alleges as follows:

INTRODUCTION

1. Representative Plaintiff John Laird ("Laird" or "Representative Plaintiff") brings this class action against Defendant Hello Housing ("Defendant") for its failure to properly secure and safeguard Representative Plaintiff's and Class Members' personally identifiable information stored within Defendant's information network, including, without limitation, medical information and health insurance information (this type of information, *inter alia*, being hereafter referred to, collectively, as "personal health information" or "PHI"),[1] full names, mailing addresses, Social Security numbers, dates of birth, driver's license or state identification information, passports, and financial information (these latter types of information, *inter alia*, being hereafter referred to, collectively, as "personally identifiable information" or "PII"),[2] and to properly secure and safeguard Representative Plaintiff's and Class Members' PHI and PII stored within Defendant's information network.

2. With this action, Representative Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiff and the countless other similarly situated persons in the massive and preventable cyberattack reported on December 2, 2020, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PHI/PII and financial information which was being kept unprotected (the "Data Breach").

[1] Personal health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

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

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

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

4. While Defendant claims to have known about the Data Breach as early as December 2, 2020, it did not immediately report the security incident to Representative Plaintiff. Indeed, Representative Plaintiff was wholly unaware of the Data Breach until he began researching potential causes of rampant identity theft he was experiencing. Because he had not provided this sensitive information to any other organization, he determined Hello Housing was a likely culprit and confirmed that it had indeed announced a data breach.

5. Defendant acquired, collected, and stored Representative Plaintiff's and Class Members' PHI/PII and/or financial information in connection with the application for services from Defendant. Therefore, at all relevant times, Defendant knew, or should have known, that it was storing Representative Plaintiff's and Class Members PHI/PII as it requested or otherwise collected this information in the course of its business.

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

7. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained

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

by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

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

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

JURISDICTION AND VENUE

10. This Court has jurisdiction over Representative Plaintiff's and Class Members' claims for damages and injunctive relief pursuant to, *inter alia*, Cal. Civ. Code §56, *et seq*., §1798, *et seq*. and Cal. Bus. & Prof. Code §17200, *et seq.*, among other California state statues.

11. Venue as to Defendant is proper in this judicial district pursuant to California Code of Civil Procedure § 395(a). Defendant provided the aforementioned services within this County to numerous Class Members and transacts business, has agents, and is otherwise within this

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

Court's jurisdiction for purposes of service of process. The unlawful acts alleged herein have had a direct effect on Representative Plaintiff and those similarly situated within the State of California and within this County.

PLAINTIFF

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

13. Prior to the Data Breach, Representative Plaintiff provided information to Defendant and connection with his application for services therefrom. As a result, Representative Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

14. At all times herein relevant, Representative Plaintiff is and was a member of the Class.

15. As required in order to receive services from Defendant, Representative Plaintiff provided Defendant with highly sensitive personal, financial, and health information.

16. Representative Plaintiff's PHI/PII was exposed in the Data Breach because Defendant stored and/or shared Representative Plaintiff's PHI/PII and financial information. His PHI/PII and financial information was within the possession and control of Defendant at the time of the Data Breach.

17. Following his providing information to Defendant, Representative Plaintiff has experienced a slew of identity theft issues. For example, his name and information was associated with several car loan applications which he did not initiate. Additionally, an unknown individual attempted to open a Target debit card in his name and did create a Costco membership in his name. Representative Plaintiff alleges, upon information and belief, that the individual(s) responsible for these acts of identity theft obtained the predicate information from Hello Housing's network.

18. As a result, Representative Plaintiff spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-

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

monitoring his accounts, and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

19. Representative Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PHI/PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining health services, which was compromised in and as a result of the Data Breach.

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

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

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

DEFENDANT

23. Defendant is a California non-profit organization that develops affordable housing. It also provides down payment assistance and assists in the building of Accessory Dwelling Units.

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

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 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

CLASS ACTION ALLEGATIONS

25. Representative Plaintiff brings this action individually and on behalf of all persons similarly situated and proximately damaged by Defendant's conduct including, but not necessarily limited to, the following Plaintiff Class:

> "All individuals within the State of California whose PHI/PII and/or financial information was stored by Defendant and was exposed to unauthorized third parties as a result of the data breach discovered on December 2, 2020."

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

27. Representative Plaintiff reserves his right to request additional subclasses be added, as necessary, based on the types of PHI/PII and financial information that were compromised and/or the nature of certain Class Members' relationship(s) to the Defendant. At present, Class Members include, *inter alia*, current and former California employees and clients of Defendant.

28. Representative Plaintiff reserves the right to amend the above definition in subsequent pleadings and/or motions for class certification.

29. This action has been brought and may properly be maintained as a class action under California Code of Civil Procedure § 382 because there is a well-defined community of interest in the litigation and the proposed class is easily ascertainable.

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

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

1) Whether Defendant engaged in the wrongful conduct alleged herein;

2) Whether Defendant had a legal duty to Representative Plaintiff and Class Members to exercise due care in collecting, storing, using and/or safeguarding their PHI/PII and financial information;

3) Whether Defendant knew or should have known of the susceptibility of Defendant's data security systems to a data breach;

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

5) Whether Defendant's failure to implement adequate data security measures, including the sharing of Representative Plaintiff's and Class Members' PHI/PII and financial information allowed the Data Breach to occur and/or worsened its effects;

6) Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

7) Whether Defendant adequately, promptly, and accurately informed Representative Plaintiff and Class Members that their PHI/PII and financial information had been compromised;

8) How and when Defendant actually learned of the Data Breach;

9) Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Representative Plaintiff and Class Members;

10) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of these systems, resulting in the loss of the PHI/PII and financial information of Representative Plaintiff and Class Members;

11) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

12) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach and/or damages flowing therefrom;

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

13) Whether Defendant's actions alleged herein constitute gross negligence and whether the negligence/recklessness of any one or more individual(s) can be imputed to Defendant;

14) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI/PII and financial information of Representative Plaintiff and Class Members;

15) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct and, if so, what is necessary to redress the imminent and currently ongoing harm faced by Representative Plaintiff, Class Members, and the general public;

16) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

17) Whether Defendant continue to breach duties to Representative Plaintiff and Class Members.

c. Typicality: The Representative Plaintiff's claims are typical of the claims of the Plaintiff Class. Representative Plaintiff and all members of the Plaintiff Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein. The same event and conduct that gave rise to Representative Plaintiff's claims are identical to those that give rise to the claims of every Class Member because Representative Plaintiff and each Class Member had his/her sensitive PHI/PII and/or financial information compromised in the same way by the same conduct of Defendant. Representative Plaintiff and all Class Members face the identical threats resulting from the breach of his/her PHI/PII and/or financial information without the protection of encryption and adequate monitoring of user behavior and activity necessary to identity those threats.

d. Adequacy of Representation: Representative Plaintiff is an adequate representative of the Plaintiff Class in that Representative Plaintiff has the same interest in the litigation of this case as the remaining 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 class in its entirety. Representative Plaintiff anticipates no management difficulties in this litigation. Representative Plaintiff and his counsel will fairly and adequately protect the interests of all Class Members.

e. Superiority of Class Action: The damages suffered by individual Class Members, are significant, but may be small relative to the enormous expense of individual litigation by each member. This

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

> makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought, by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

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 the Representative Plaintiff.

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

//

//

//

//

//

//

//

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 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COMMON FACTUAL ALLEGATIONS

The Cyberattack

32. According to Defendant's notice:[3] Defendant's investigation into unusual activity on its network, concluded that an unauthorized party had access to data stored on Defendant's information systems which stored Class Members' PHI/PII and financial information.

33. In the course of the Data Breach, one or more unauthorized third parties accessed and/or took Class Members' sensitive data including, but not limited to full names, mailing addresses, Social Security numbers, dates of birth, driver's license or state identification information, passports, medical information, health insurance information, and financial account information. Representative Plaintiff was among the individuals whose data was accessed in the Data Breach.

34. Defendant did not notify Representative Plaintiff that his information was accessed by unauthorized third parties.

Defendant's Failed Response to the Breach

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

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

[3] The sample notice Defendant provided to the California Attorney General's Office is available at https://oag.ca.gov/system/files/Midpen%20Housing%20Notification%20letter%20proof.pdf (last accessed May 26, 2022).

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

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

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

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

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

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

41. As a condition of its relationships with Representative Plaintiff and Class Members, Defendant required that Representative Plaintiff and Class Members entrust Defendant with highly sensitive and confidential PHI/PII and financial information.

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

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

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

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

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

46. Organizations and industries which store PHI have experienced a large number of high-profile cyberattacks even in just the one-year period preceding the filing of this Complaint and cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[4] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported in April 2021.[5]

47. For example, Universal Health Services experienced a cyberattack on September 29, 2020 that appears similar to the attack on Defendant. As a result of this attack, Universal Health Services suffered a four-week outage of its systems which caused as much as $67 million in recovery costs and lost revenue.[6] Similarly, in 2021, Scripps Health suffered a cyberattack, an event which effectively shut down critical health care services for a month and left numerous

[4] https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/ (last accessed November 5, 2021).
[5] https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/ (last accessed November 5, 2021).
[6] https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and (last accessed November 5, 2021).

patients unable to speak to their physicians or access vital medical and prescription records.[7] A few months later, University of San Diego Health suffered a similar attack.[8]

48. Due to the high-profile nature of these breaches, and other breaches of their kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack.

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

Defendant Had an Obligation to Protect the Stolen Information

50. Defendant's failure to adequately secure Representative Plaintiff's and Class Members' sensitive data also breaches duties it owes Representative Plaintiff and Class Members under statutory and common law. Under HIPAA, healthcare providers have an affirmative duty to keep patients' Protected Health Information private. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiff's and Class Members' data. Moreover, Representative Plaintiff and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

51. Because Defendant is covered as a Business Associate by HIPAA (45 C.F.R. § 160.102), they are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[7] https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/ (last accessed November 5, 2021).

[8] https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-accounts-impacted/2670302/ (last accessed November 5, 2021).

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

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

52. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

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

54. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

55. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

56. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

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

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

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

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

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

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

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

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

65. Defendant owed a duty to Representative Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals'

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

PHI/PII and/or financial information from theft because such an inadequacy would be a material fact in the decision to entrust this PHI/PII and/or financial information to Defendant.

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

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

Value of the Relevant Sensitive Information

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

69. The high value of PHI/PII and financial information to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[9] Experian reports

[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

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

that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[10] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[11]

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

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

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

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

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

[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed November 5, 2021).

[12] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133 (last accessed November 4, 2021).

[13] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed November 4, 2021).

[14] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed November 4, 2021).

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

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

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

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

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

76. The harm to Representative Plaintiff and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-

[15] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed November 4, 2021).

related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[16]

77. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[17]

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

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

80. And data breaches are preventable.[20] 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."[21] she added that "[o]rganizations that collect, use, store, and share sensitive

[16] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed November 4, 2021).
[17] *Id*.
[18] See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed November 4, 2021).
[19] Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed November 4, 2021).
[20] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[21] *Id.* at 17.

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

personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[22]

81. 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*."[23]

82. Here, Defendant knew, or should have known, 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 a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It 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.

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

//

//

[22] *Id.* at 28.
[23] *Id.*

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 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

FIRST CAUSE OF ACTION
Negligence

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

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

86. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII and financial information in its possession;

b. to protect Representative Plaintiff's and Class Members' PHI/PII and financial information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Representative Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PHI/PII and financial information.

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

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

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

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

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

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

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

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

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

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

b. by failing to timely and accurately disclose that Representative Plaintiff's and Class Members' PHI/PII and financial information had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PHI/PII and financial information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PHI/PII and financial information;

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

d. by failing to provide adequate supervision and oversight of the PHI/PII and financial information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PHI/PII and financial information of Representative Plaintiff and Class Members, misuse the PHI/PII and intentionally disclose it to others without consent.

e. by failing to adequately train its employees to not store PHI/PII and financial information longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff's and the Class Members' PHI/PII and financial information;

g. by failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. by failing to encrypt Representative Plaintiff's and Class Members' PHI/PII and financial information and monitor user behavior and activity in order to identify possible threats.

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

97. 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).

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

99. Defendant breached its duty to notify Representative Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Representative Plaintiff and Class Members and then by failing and continuing to fail to provide Representative Plaintiff and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiff and Class Members

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

regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiff and Class Members.

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

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

102. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

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

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

105. Defendant violated 15 U.S.C. §45 by failing to use reasonable measures to protect PHI/PII and financial information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PHI/PII and financial information it obtained and stored and the foreseeable

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

consequences of the immense damages that would result to Representative Plaintiff and Class Members.

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

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

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

109. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PHI/PII and financial information, which remain in

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

Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI/PII and financial information in its continued possession.

SECOND CAUSE OF ACTION
Confidentiality of Medical Information Act
(Cal. Civ. Code §56, *et seq*.)

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

111. Under the CMIA, California Civil Code §56.05(k), Representative Plaintiff and Class Members (except employees of Defendant whose records may have been accessed) are deemed "patients."

112. As defined in the CMIA, California Civil Code §56.05(j), Defendant disclosed "medical information" to unauthorized persons without obtaining consent, in violation of §56.10(a). Defendant's misconduct, including failure to adequately detect, protect, and prevent unauthorized disclosure, directly resulted in the unauthorized disclosure of Representative Plaintiff's and Class Members' PHI/PII and financial information to unauthorized persons.

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

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

115. Representative Plaintiff and Class Members were injured and have suffered damages, as described above, from Defendant's illegal disclosure and negligent release of their

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

PHI/PII and financial information in violation of Cal. Civ. Code §§ 56.10 and 56.101 and, therefore, seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

THIRD CAUSE OF ACTION
Breach of Implied Contract

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

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

118. Defendant required Representative Plaintiff and Class Members to provide and entrust their PHI/PII and financial information in the course of its legal work.

119. Defendant solicited and invited Representative Plaintiff, and Class Members to provide their PHI/PII and financial information as part of Defendant's regular business practices. Representative Plaintiff and Class Members accepted Defendant's offers and provided their PHI/PII and financial information to Defendant.

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

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

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

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

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

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

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

FOURTH CAUSE OF ACTION
Unfair Business Practices/Unfair Competition Act
(Cal. Bus. & Prof. Code, §17200, *et seq*.)

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

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

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

128. Representative Plaintiff, the Class Members, and Defendant are each a "person" or "persons" within the meaning of § 17201 of the California Unfair Competition Law ("UCL").

129. The knowing conduct of Defendant, as alleged herein, constitutes an unlawful and/or fraudulent business practice, as set forth in California Business & Professions Code

§§17200-17208. Specifically, Defendant conducted business activities while failing to comply with the legal mandates cited herein, including HIPAA. Such violations include, but are not necessarily limited to:

a. failure to maintain adequate computer systems and data security practices to safeguard PHI/PII and financial information;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard PHI/PII and financial information from theft;

c. failure to timely and accurately disclose the Data Breach to Representative Plaintiff and Class Members;

d. continued acceptance of PHI/PII and financial information and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. continued acceptance of PHI/PII and financial information and storage of other personal information after Defendant knew or should have known of the Data Breach and before it allegedly remediated the Data Breach.

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

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

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

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

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

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

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

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

RELIEF SOUGHT

WHEREFORE, Representative Plaintiff, on behalf of himself and each member of the proposed Class, respectfully requests that the Court enter judgment in his/their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify the proposed class and/or any other appropriate subclasses under California Code of Civil Procedure § 382;

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

3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities in further violation of California Business and Professions Code §17200, *et seq*.;

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

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

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

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiff's and Class Members' PHI/PII and financial information;

d. 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;

e. prohibiting Defendant from maintaining Representative Plaintiff's and Class Members' PHI/PII and financial information on a cloud-based database;

f. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's networks are compromised, hackers cannot gain access to other portions of Defendant's systems;

g. requiring Defendant to conduct regular database scanning and securing checks;

h. 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 and financial information, as well as protecting the PHI/PII and financial information of Representative Plaintiff and Class Members;

i. 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 PHI/PII and financial information;

j. 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;

k. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

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

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 sought in this Complaint.

JURY DEMAND

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

Dated: May 26, 2022

COLE & VAN NOTE

By: _____
Cody A. Bolce, Esq.
Attorneys for Representative Plaintiff
and the Plaintiff Class

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