BARRACK, RODOS & BACINE
STEPHEN R. BASSER (SBN 121590)
SAMUEL M. WARD (SBN 216562)
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874
sbasser@barrack.com
sward@barrack.com

Counsel for Plaintiff Darleen Perez
Additional Counsel Identified on Signature Page

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF LOS ANGELES

DARLEEN PEREZ, on behalf of herself, and on behalf of all others similarly situated,

Plaintiff,

v.

KEENAN & ASSOCIATES,

Defendant.

Case No. 24STCV04704

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1. Negligence
2. Negligence *Per Se*
3. Breach of Implied Covenant of Good Faith and Fair Dealing
4. Breach of Fiduciary Duty
5. Breach of Duty
6. Breach of Implied Contract
7. Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*
8. Invasion of Privacy,Cal. Const. Art. 1 § 1
9. California Unfair Competition Law Cal. Bus. & Prof. Code, § 17200, *et seq.*
10. Violation of California Consumer Records Act, Cal. Civ. Code § 1798.82, *et seq.*
11. Violation of California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.*

Plaintiff Darleen Perez ("Perez" or "Plaintiff"), by and through her attorneys of record, upon personal knowledge as to her own acts and experiences, upon the investigation of counsel, and upon information and belief as to all other matters, brings this class action complaint against defendant Keenan & Associates ("Keenan" or "Defendant"), and alleges as follows:

INTRODUCTION

1. Plaintiff brings this class action on behalf of a Class, as defined below, against Defendant for its failure to properly secure and safeguard Plaintiff's and Class Members' protected personal information stored within Defendant's information networks and servers, including, without limitation, "protected health information" ("PHI"),[1] and "personally identifiable information" ("PII"),[2] as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, PHI and PII are also referred to therein as "Private Information").

2. Defendant is an insurance brokerage company that provides risk management and claims services throughout the country. In the course of providing these services, Keenan was provided with the Private Information of Plaintiff and the Class. Keenan represents that it is the eleventh largest insurance broker in the United States.[3]

3. In the course of providing mortgages to consumers and class members, Defendant acquired and collected Plaintiff's and Class Members' Private Information. Defendant knew, at all times material, that it was collecting, and responsible for the security of, sensitive data,

---

[1] Protected 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. PHI is inclusive of and incorporates personally identifiable information.

[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 its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[3] https://www.keenan.com/ last visited on February 20, 2024.

including Plaintiff's and Class Members' highly confidential Private Information. This Private Information remains in the possession of Defendant, despite the fact that it was accessed by unauthorized third persons and is currently being maintained without appropriate and necessary safeguards, independent review, and oversight, and therefore remains vulnerable to additional hackers and theft.

4. Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and approximately 1.5 million other similarly situated persons by virtue of a massive and preventable cyberattack that Defendant discovered no later than August 27, 2023, when Keenan "discovered certain interruptions occurring on some Keenan network servers " and immediately began an investigation[.]"[4] Defendant contends that "[w]ithin hours of identifying the cybersecurity incident, we had contained it."[5] As set forth in the notice that Defendant began sending to Plaintiff and class members no sooner than January 26, 2024 (the "Notice of Data Breach"), Defendant determined that between "approximately August 21, 2023 and August 27, 2023," hackers "obtained some data from Keenan systems[,]" including "your name, date of birth, Social Security number, driver's license number, passport number, general health information, and health insurance information." (the "Data Breach"). Remarkably, Keenan failed to begin notifying Plaintiff and the Class of the Data Breach until late January, 2024, approximately five months after discovering the Data Breach. Plaintiff further seeks to hold Defendant responsible for not ensuring that the Private Information was maintained in a manner consistent with industry standards.

5. Plaintiff further seeks to hold Defendant responsible for not ensuring that PII and PHI, as defined by HIPAA Privacy Rule (45 CFR, Parts 160 and 164(A) and (E)), and respecting which Defendant was duty bound to protect pursuant to the HIPAA Security Rule (45 CFR, Parts 160 and 164(A) and (C)), was maintained in a manner consistent with industry standards, and other relevant standards.

6. HIPAA, in general, applies to healthcare providers, health plans/insurers, health care clearinghouses, those health care providers that conduct certain health care transactions

---

[4] https://www.keenan.com/Notice-of-Security-Incident, last visited on February 21, 2024.

[5] *Id.*

electronically, and HIPAA Business Associates, and sets standards for Defendant's maintenance of Plaintiff's and Class Members' PII and PHI, including appropriate safeguards to be maintained by organizations such as Defendant's to protect the privacy of patient health information, while setting limits and conditions on the uses and disclosures that may be made of such information without express customer/patient authorization.

7. Additionally, the so-called "HIPAA Security Rule" establishes national standards to protect individuals' electronic health information that is created, received, used, or maintained by a HIPAA Business Associate. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI. HIPAA provides the standard of procedure by which a medical provider must operate when collecting, storing, and maintaining the confidentiality of PHI and PII.

8. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant knowingly assumed legal and equitable duties to those individuals, including those arising from common law principles.

9. Nonetheless, Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take, implement, and ensure adequate and reasonable measures regarding the safeguarding of Plaintiff's and Class Members' PII and PHI, 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. As a result and upon information and belief, the PII and PHI of Plaintiff and Class Members has been compromised and they have been and shall be damaged through access by and disclosure to an unknown and unauthorized entity—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future. In addition, Plaintiff and Class Members, who have a continuing interest in ensuring that their information is safe, are entitled to injunctive and other equitable relief.

PARTIES

Plaintiff

10. Plaintiff Darleen Perez is, and at all relevant times was, a resident of Long Beach, Los Angeles County, California. On or about February 6, 2024, Plaintiff Perez received the Notice of Data Breach. Prior to receiving the Notice of Data Breach, Plaintiff Perez was unaware that her Private Information had been exfiltrated and had no notice prompting her to take additional steps to protect herself from financial fraud or identity theft. Plaintiff Perez takes care to protect her Personal Information from public disclosure. Shortly after the Data Breach, in early October 2023, Perez received notice of several attempted fraudulent transactions relating to her checking account in which an unknown actor, apparently located in Spain, attempted to purchase event tickets costing hundreds of dollars. Since receiving the Notice of the Data Breach, Plaintiff has been forced to spend uncompensated time monitoring personal financial accounts for signs of fraudulent transactions or activity and anticipates that she will continue to have to do so.

Defendant

11. Keenan is an insurance brokerage company that provides risk management and claims services throughout California and to its clients across the country. These services include, *inter alia*, managing employee benefits packages and third party claims services for workers' compensation claims. Keenan provides these services to insurance companies and, in the course of providing these services, was provided with the Private Information of Plaintiff and the Class. Keenan maintains offices throughout California, including an office located at 111 Broadway, Suite 2000, Oakland, California.

JURISDICTION AND VENUE

12. This Court has jurisdiction over this action under California Code of Civil Procedure § 410.10. The total amount of aggregate damages incurred by Plaintiff and the Class exceeds the $25,000 jurisdictional minimum of this Court. Further, upon information and belief,

the amount in controversy as to Plaintiff individually does not exceed $75,000. Upon information and belief, more than 2/3 of the proposed Class are citizens and residents of California.

13. Venue is proper in this Court under California Bus. & Prof. Code § 17203 and Code of Civil Procedure §§ 395(a) and 395.5 because Defendant and/or its parents or affiliates are headquartered in this judicial district and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this judicial district.

14. This Court is the proper venue for this action because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District, and because Defendant conducts a substantial part of their business within this District.

FACTUAL BACKGROUND

The Data Breach

15. The Data Breach occurred when one or more unauthorized third parties accessed Keenan's computer network on which the Private Information of Plaintiff and the Class were stored. On or about January 26, 2024, Defendant posted a notice, accessible via a link on its homepage, indicating that, no later than August 27, 2023, Defendant "discovered certain interruptions occurring on some Keenan network servers "and immediately began an investigation[.]"[6] Defendant contends that "[w]ithin hours of identifying the cybersecurity incident, we had contained it."[7]

16. On January 26, 2024, the Company began sending the Notice of Data Breach to Plaintiff and the Class. In the Notice of Data Breach, Defendant determined that between "approximately August 21, 2023 and August 27, 2023," hackers "obtained some data from Keenan systems[,]" including "your name, date of birth, Social Security number, driver's license number, passport number, general health information, and health insurance information." Defendant has provided no explanation as to why it failed to begin notifying Plaintiff and the Class of the Data Breach until late January, 2024, approximately five months after discovering the Data Breach.

---

[6] https://www.keenan.com/Notice-of-Security-Incident, last visited on February 21, 2024.

[7] *Id.*

17. The "disclosure," of the Data Breach, coming five months after Defendant discovered the Data Breach, amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

18. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, and failed to adhere to the standard of care required of healthcare related business and services, ultimately leading to and causing the exposure of Private Information.

19. Upon information and belief, the exfiltrated data was not encrypted or hashed, allowing nefarious actors easy access to the data.

20. Upon information and belief, Defendant continues to inadequately secure or maintain Plaintiff's PHI and PII, as well as that of all other Class Members.

21. Beyond acknowledging the Data Breach – albeit inadequately – Defendant's therapeutic steps are inadequate. Defendant has failed to adequately compensate Plaintiff and members of the Class. Defendant has failed to adequately address the multiple years of identity theft and financial fraud that Data Breach victims face. As a consequence of the Data Breach, Plaintiff and Class Members will be forced to pay out-of-pocket for necessary identifying monitoring services for years thereafter.

Keenan is Obliged to Preserve and Protect PHI and PII

22. Defendant acquired, collected, stored, and assured the security of, the Private Information of Plaintiff and the Class.

23. As a consequence of securing or receiving insurance and/or having claims processed, Plaintiff and Class Members were required to provide sensitive and confidential Private Information, including their names and Social Security Numbers, and other sensitive information, to Defendant.

24. Defendant was entrusted with the Private Information of more than a million patients. Keenan maintains a "Privacy Policy" (the "Privacy Policy") setting forth its

understanding of its obligations to safeguard and protect the confidentiality of consumers Private Information.[8]

25. In its Privacy Policy, Keenan asserts that it "respects your privacy and takes our privacy responsibility very seriously and is committed to protecting it in a manner consistent with applicable law and this statement."[9] Keenan further represents that it has "implemented measures reasonably designed to protect and secure your Personal Information from accidental loss, misuse, and from unauthorized access, use, alteration, and disclosure."[10]

26. Plaintiff and Class Members provided their Private 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. The information collected, acquired, and stored by Defendant included the Private Information of Plaintiff and Class Members.

27. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members, who value the confidentiality of their Private Information and demand security to safeguard their Private Information, took reasonable steps to maintain the confidentiality of their PII/PHI.

28. At all times material, Defendant was under a duty to adopt and implement reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. To that end, Defendant was reposed with a legal duty created by HIPAA, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

---

[8] https://www.keenan.com/Privacy-Statement (last visited on February 20, 2024.)

[9] *Id.*

[10] *Id.*

29. By obtaining, collecting, using, and storing Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties, and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure. And given the highly sensitive nature of the PII and PHI it possessed and the sensitivity of the medical and health services it provides, Defendant had a duty to safeguard, protect, and encrypt Plaintiff's and Class Members' PII and PHI.

30. Defendant retains and stores this Private Information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to perform its services.

31. Defendant's failure to adequately safeguard the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

32. Defendant was not permitted to disclose Plaintiff's and Class Members' Private Information for any reason that would apply in this situation.

33. Defendant was obliged by contract, industry standards, common law, and promises and representations made to Plaintiff and Class Members, to keep their Private Information confidential and protect it from unauthorized access and disclosure.

34. Plaintiff and Class Members had a reasonable expectation and mutual understanding that Defendants would comply with its obligations to keep the Private Information they provided confidential and secure from unauthorized access and disclosure.

35. Defendants failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, consequently enabling and causing the exposure of Private Information of approximately 1.5 million individuals.

36. Because of Defendant's negligence and misconduct in failing to keep the accessed information confidential, the unencrypted Private Information of Plaintiff and Class Members has been expropriated by unauthorized individuals who can now exploit the PHI and PII of Plaintiff and Class Members and use it as they please.

37. Even though Defendants recognized no later than August 27, 2023, that its computer network had been breached, it delayed sending written notice directly to members of the Class.

38. Plaintiff and Class Members now face a real, present and substantially increased risk of fraud and identity theft and have lost the benefit of the bargain they made with Defendant when receiving services.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

39. The PII and PHI of consumers, such as Plaintiff and Class Members, is highly valuable and has been commoditized in recent years.

40. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer both immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

41. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. They must now be vigilant and continuously review their credit reports for suspected incidents of identity theft, educate themselves about security freezes, fraud alerts, and take steps to protect themselves against identity theft, which will extend indefinitely into the future.

42. Plaintiff and Class Members also suffer ascertainable losses in the form of opportunity costs and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to the information in possession of Defendants;

C. Purchasing credit monitoring and identity theft prevention;

D. Addressing their inability to withdraw funds linked to compromised accounts;

E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

G. Placing freezes and alerts with credit reporting agencies;

H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

L. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

43. Moreover, Plaintiff and Class Members have an interest in ensuring that Defendants implement reasonable security measures and safeguards to maintain the integrity and confidentiality of the Private Information, including making sure that the storage of data or documents containing Private Information is not accessible by unauthorized persons, that access to such data is sufficiently protected, and that the Private Information remaining in the possession of Defendants is encrypted, fully secure, remains secure, and is not subject to future theft.

44. As a further direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

45. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized access of and disclosure or risk of exfiltration of Plaintiff's and Class Members' Private Information, Plaintiff and Class Members have suffered, and will continue to suffer, actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they have spent or must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; and (iii) emotional distress as a result of having their Private Information accessed by unauthorized cyber-thieves in the Data Breach.

Defendant was Well Aware of the Threat of Cyber Theft and Exfiltration in the Healthcare Industry

46. Defendant was aware of the significant repercussions that would result from their failure to protect Private Information and knew, or should have known, the importance of safeguarding the Private Information entrusted to them and of the foreseeable consequences of a breach of data security.

47. Defendants could have prevented the Data Breach by assuring that the Private Information at issue was properly secured. Defendant's overt negligence in safeguarding Plaintiff's and Class Members' PII and PHI is exacerbated by repeated warnings and alerts directed at protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as entities in the healthcare space, Defendant was on notice that companies in the healthcare industry are targets for data breaches.

48. The healthcare industry in particular has experienced a large number of high-profile cyberattacks. Cyberattacks, generally, have become increasingly more common. In 2021, a record 715 healthcare data breaches reported, an increase of approximately 100% since 2017.[11]

[11] 2022 Healthcare Data Breach Report, https://www.hipaajournal.com/2022-healthcare-data-breach-report/ (last accessed February 20, 2024).

49. This trend continued in 2022, with 707 healthcare breaches reported, still near record highs.[12] Additionally, according to the HIPAA Journal, the five largest healthcare data breaches reported in 2022 impacted the healthcare records of approximately 13.3 million people.[13] Thus, Defendant was on further notice regarding the increased risks of inadequate cybersecurity. In February 2022, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic rise in cyberattacks, including ransomware attacks, urging facilities to shore up their cyber defenses.[14] Indeed, HHS's cybersecurity arm has issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[15]

50. In the context of data breaches, healthcare is "by far the most affected industry sector."[16] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[17]

51. A TENABLE study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in nearly 93% of the breaches."[18]

---

[12] *Id.*

[13] *Id.*

[14] Rebecca Pifer, Tenet says 'cybersecurity incident' disrupted hospital operations, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-sayscybersecurity-incident-disrupted-hospital-operations/622692/ (last accessed February 20, 2024).

[15] *Id.* (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June - nearly three a day.").

[16] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed February 20, 2024).

[17] *Id.*

[18] *Id.*

52. This is such a breach of cybersecurity where highly detailed PII and PHI records maintained and collected by a healthcare entity were accessed and/or acquired by a cybercriminal.

53. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendants are large, sophisticated operations with the resources to put adequate data security protocols in place and assure the security of the data collected by them and entrusted to them by Plaintiff and Class Members.

54. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiff's and Class Members' PII and PHI from being compromised.

Defendant's Conduct Fails to Adhere to Industry Standards, HIPAA and HITECH Standards, and Commensurate Duties it Owed to Plaintiff and the Class

55. Defendants embraced a standard of care and commensurate duty defined by HIPAA, state law and common law to safeguard the PHI and PII of Plaintiff and Class Members data.

56. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data under the condition and implied promise and assurance by Defendants that they would keep such Private Information confidential and secure. Accordingly, Defendants also had an implied duty to safeguard their data, independent of any statute.

57. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

58. On information and belief, Defendant is a business associate pursuant to HIPAA.

59. Defendants are also regulated by the Health Information Technology Act ("HITECH").[19] See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

60. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is 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.

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

62. 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.

63. 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.

64. "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.

65. HIPAA's Security Rule requires Defendants 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;

[19] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

c) Protect Against reasonably anticipated uses or disclosures of such information that are not permitted; and

d) Ensure compliance by its workforce.

66. HIPAA also requires Defendants 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).

67. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendants 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."

68. Plaintiff's and Class Members' Personal and Medical Information, including their PII and PHI, is "protected health information" as defined by 45 CFR § 160.103.

69. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

70. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

71. Plaintiff's and Class Members' personal and medical information, including their PII and PHI, is "unsecured protected health information" as defined by 45 CFR § 164.402.

72. Plaintiff's and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

73. Plaintiff's and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

74. Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

75. Plaintiff's and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

76. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

77. HIPAA requires covered entities and business associates to protect against reasonably anticipated threats to the security of sensitive patient health information.

78. Covered entities and business associates must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

79. This Data Breach constitutes an unauthorized access of PHI, which is not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

80. The Data Breach could have been prevented if Defendants had implemented HIPAA mandated and industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients with respect to adequately securing and maintaining the confidentiality of Private Information.

81. It can be inferred from the Data Breach that Defendants either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Representative Plaintiff's and Class Members' PII and PHI.

82. Upon information and belief, prior to the Breach, Defendant was aware of its security failures but failed to correct them or adequately and timely disclose them to the public, including Plaintiff and Class Members.

83. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendants knew or should have known that they did not make such actions and failed to implement adequate data security practices.

84. Because Defendants failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendants still maintain the PII and PHI of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff's and Class Members' PII and PHI remains at risk of subsequent Data Breaches.

85. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to 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 Private Information of Plaintiff and Class Members.

86. Defendants owed a duty to Plaintiff and Class Members to ensure that the Private Information they collected and were responsible for was adequately secured and protected.

87. Defendants owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in their possession, including not sharing information with other entities who maintained sub-standard data security systems.

88. Defendants owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach that impacted the Private Information it collected and was responsible for in a timely manner.

89. Defendants owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

90. Defendants owed a duty to Plaintiff and Class Members to disclose if their data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust this Private Information to Defendants.

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

92. Defendants owed a duty to Plaintiff and Class Members to mitigate the harm suffered by the Representative Plaintiff's and Class Members' as a result of the Data Breach.

93. Upon information and belief, Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system and safeguards to prevent data loss;
b. Failing to mitigate the risks of a data breach and loss of data, including identifying internal and external risks of a security breach;
c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants creates, receives, maintains, and transmits;
d. Failing to implement 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;
e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;
g. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information;
h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information;

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons; and

k. Retaining information past a recognized purpose and not deleting it.

The Federal Trade Commission Defines Defendant's Conduct as Constituting Unfair or Deceptive Acts

94. The Federal Trade Commission ("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 Corp.*, 799 F.3d 236 (3d Cir. 2015).

95. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

96. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, encrypt information stored on networks, understand its network's vulnerabilities, and implement policies to correct any security problems.[21]

97. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

98. Defendants failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice.

---

[20] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf last visited February 20, 2024).

[21] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business last visited February 20, 2024.

99. Defendant was at all times fully aware of its obligations to protect Plaintiff's and Class Members' Private Information because of their business models of collecting and storing Private Information. Defendant was also aware of the significant adverse repercussions befalling healthcare recipients that would result from its failure to do so.

Value of the Relevant Sensitive Information

100. Although they provide greater efficiency and cost savings for providers, 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 seeking to access them. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PII and PHI 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. Unsurprisingly, the healthcare industry is at high risk for and acutely affected by cyberattacks.

101. The high value of PII and PHI 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.[22] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[23]

102. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[24] Indeed, during 2019 alone, over 41 million healthcare records were exposed,

---

[22] 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-darkweb-how-much-it-costs/ last accessed February 20, 2024.

[23] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ last visited February 20, 2024.

[24] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133 last visited February 20, 2024.

stolen, or unlawfully disclosed in 505 data breaches.[25] 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.[26]

103. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members. For example, it is believed that certain 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 Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

104. 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."

105. Identity thieves can use PII and PHI and financial information, such as that of Plaintiff and Class Members, which Defendants 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.

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

---

[25] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ last visited February 20, 2024.

[26] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches last visited February 20, 2024.

> [L]aw enforcement officials told us that in some cases, stolen data may be held 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.[27]

107. The harm to 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- 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.[28]

108. "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."[29]

109. 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 Defendants may have exposed Plaintiff and Class Members.

110. 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.[30] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while

---

[27] 47 Report to Congressional Requesters, GAO, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf last visited February 20, 2024.

[28] 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 visited February 20, 2024.

[29] *Id.*

[30] 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 visited February 20, 2024.

nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[31]

111. Data breaches are preventable.[32] 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."[33] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[34]

112. 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*."[35]

113. The Data Breach resulted from a combination of insufficiencies that demonstrate how Defendants failed to comply with industry, standards, safeguards and concomitant duties established by HIPAA regulations.

114.

Loss of the Benefit of the Bargain

115. As a consequence of Defendant's inadequate data security systems and protection, Plaintiff and Class Members have been deprived of the benefit of their bargain which occurred when they agreed to receive services administered by Defendant. Plaintiff and Class Members, reasonable consumers – understandably expected that they were, in part, paying for the service

---

[31] *Id.; see also* Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, available at https://www.experian.com/blogs/ask-experian/healthcare-data-breachwhat-to-know-about-them-and-what-to-do-after-one/ last visited February 20, 2024.

[32] Lucy L. Thompson, Despite the Alarming Trends, Data Breaches Are Preventable, in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[33] *Id.* at 17.

[34] *Id*. at 28.

[35] *Id.*

and necessary data security to protect the Private Information when, in fact, Defendants had not provided the necessary adequate data security in any event. Consequently, Plaintiff and Class Members received services that were of a lesser value than what they had reasonably expected from and bargained for with Defendant.

Ongoing Need for Expensive Credit and Identity Theft Monitoring

116. Unquestionably there will be a future cost of credit and identify theft monitoring that will be necessary for Plaintiff and Class Members' protection going forward as a consequence of the Data Breach and the sensitive Private Information that has been accessed. The probability is strong that the stolen information will be used by criminals to accomplish crimes based on identity theft, including opening bank accounts and victims' names to make purchases or launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims. These fraudulent incidents may not be detected for years and individuals may not even know that they have yet occurred.

117. Credit monitoring and identity theft monitoring is expensive. The cost can run approximately $200 a year per each Class Member. This cost is necessary and reasonable, for Plaintiff and Class Members are now forced to monitor and protect themselves from identity theft going forward, and need to do so for many years.

Defendant's Inadequate Response to the Breach

118. Time is of the essence when highly sensitive PII and PHI is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII and PHI of Plaintiff and Class Members is likely available, or may be available at any moment, on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII and PHI, especially their Social Security numbers and sensitive medical information, onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure,

and/or activity by cybercriminals on computer systems containing Social Security numbers, Dates of birth, and other critical PHI and/or PII.

119. Despite this understanding, Defendants have not made adequate and timely written notice of the Data Breach to Plaintiff and Class Members and has provided only scant details.

120. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.8% of U.S.-based workers are compensated on an hourly basis, while the other 44.2% are salaried.[36]

121. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[37] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[38] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

122. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

CLASS ALLEGATIONS

---

[36] U.S. BUREAU OF LABOR STATISTICS, Characteristics of minimum wage workers, 2021, available at https://www.bls.gov/opub/reports/minimum-wage/2021/pdf/home.pdf, last visited February 20, 2024; *see also*, Bureau of Labor Statistics, https://www.bls.gov/news.release/empsit.t19.htm, last visited February 20, 2024 (finding that on average, private-sector workers make $1,146.99 per 40-hour work week).

[37] See https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html last visited February 20, 2024.

[38] *Id.*

123. Pursuant to California Code of Civil Procedure § 382, Plaintiff assert common law claims, as more fully alleged hereinafter, on behalf of the following on behalf of the following Nationwide Class and California Class (collectively "the Class"):

> **Nationwide Class**: All residents of the United States whose PII or PHI was accessed or otherwise compromised as a result of the Data Breach.
>
> **California Class:** All residents of the state of California whose PII or PHI was accessed or otherwise compromised as a result of the Data Breach.

Members of the Class are referred to herein collectively as "Class Members" or "Class."

124. Excluded from the Class are Defendants, any entity in which Defendants have a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

125. **Numerosity**: The exact number of members of the Class is unknown to Plaintiff at this time but Keenan provides services to over one million consumers and has acknowledged that the number of individuals affected by the Data Breach was approximately 1.5 million persons, indicating that joinder of all members of the Class is impracticable. Ultimately, members of the Class will be readily identified through Defendant's records.

126. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendants failed to adequately safeguard Plaintiff's and the Class Members' PII and PHI;

b) Whether Defendants failed to protect Plaintiff's and the Class Members' PII and PHI, as promised;

c) Whether Defendant's computer systems and data security practices used to protect Plaintiff's and the Class Members' PII and PHI violated state and local laws, or Defendant's duties;

d) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and the Class Members' PII and PHI properly and/or as promised;

e) Whether Defendants violated the consumer protection statutes, data breach notification statutes, state unfair practice statutes, state privacy statutes, and state medical privacy statutes, HIPAA, and/or regulations, imposing duties upon Defendants, applicable to Plaintiff and Class Members;

f) Whether Defendants failed to notify Plaintiff and members of the Class about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

g) Whether Defendants acted negligently in failing to safeguard Plaintiff's and the Class Members' PII and PHI;

h) Whether Defendants entered into contracts with Plaintiff and the Class Members that included contract terms requiring Defendants to protect the confidentiality of Plaintiff's PII and PHI and have reasonable security measures;

i) Whether Defendant's conduct described herein constitutes a breach of contracts with Plaintiff and each of the Class Members;

j) Whether Defendants should retain any money paid by Plaintiff and each of the Class Members to protect their PII and PHI;

k) Whether Plaintiff and the Class Members are entitled to damages as a result of Defendant's wrongful conduct;

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

m) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Class Members.

127. **Typicality**: Plaintiff's claims are typical of the claims of each of the Class Members. Plaintiff and the Class Members sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

128. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff Perez and her counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and has the financial resources to do so. Neither Plaintiff Perez nor her counsel have any interest adverse to those of the other members of the Class.

129. **Separateness**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendants or would be dispositive of the interests of members of the proposed Class. Furthermore, the Private Information collected by Defendants still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the PHI and PII collected, stored, and maintained by Defendants.

130. **Class-wide Applicability**: This case is appropriate for certification because Defendants has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

131. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of

the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendants. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

COUNT I

Negligence
(On Behalf of Plaintiff and the Class)

132. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

133. Plaintiff and Class Members were required to submit PII and PHI to Defendant in order to obtain services.

134. Defendants knew, or should have known, of the risks and responsibilities inherent in collecting and storing the PII and PHI of Plaintiff and Class Members.

135. As described above, Defendants owed a duty of care to Plaintiff and Class Members whose PII and PHI had been entrusted to Defendants.

136. Defendants breached its duty to Plaintiff and Class Members by failing to secure their PII and PHI from unauthorized disclosure to third parties.

137. Defendants acted with wanton disregard for the security of Plaintiff's and Class Members' PII and PHI.

138. A "special relationship" exists between Defendants and the Plaintiff and Class Members. Defendants entered into a "special relationship" with Plaintiff and Class Members because it collected and/or stored the PII and PHI of Plaintiff and the Class Members.

139. But for Defendant's wrongful and negligent breach of its duty owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

140. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duty. Defendant knew or should have known it was failing to meet its duty, and that Defendant's breach of its duty would cause Plaintiff and Class Members to experience the foreseeable harms associated with the unauthorized exposure of their PII and PHI.

141. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II

Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

142. Plaintiff, on behalf of herself, and the Class, re-alleges and incorporates the above allegations by reference.

143. Defendants had a legal duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PII and PHI.

144. Defendants breached its duty to Plaintiff and Class Members by failing to implement reasonable safeguards to protect Plaintiff's and Class Members' PII and PHI from unauthorized access.

145. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

146. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

147. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duty. Defendants knew or should have known that it was failing to meet its duty, and that Defendant's breach of that duty would cause Plaintiff and Class Members to experience the foreseeable harms associated with the unauthorized access to their PII and PHI.

148. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III

Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and the Class)

149. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

150. Plaintiff and Class Members entered into valid, binding, and enforceable express or implied contracts with entities affiliated with or serviced by Defendants, as alleged above.

151. The contracts respecting which Plaintiff and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform its contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendants would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiff's PII and PHI from unauthorized disclosure and to comply with state laws and regulations.

152. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members who received services related to the provision of healthcare from Defendant and, in doing so, entrusted Defendant, pursuant to their requirements, with PII and PHI.

153. Despite this special relationship with Plaintiff, Defendant did not act in good faith and with fair dealing to protect Plaintiff's and Class Members' PII and PHI.

154. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Defendants.

155. Defendant's failure to act in good faith in complying with the contracts denied Plaintiff and Class Members the full benefit of their bargain, and instead they received services that were less valuable than what they paid for and less valuable than their reasonable expectations.

156. Accordingly, Plaintiff and Class Members have been injured as a result of Defendant's breach of the covenant of good faith and fair dealing respecting which they are express

or implied beneficiaries, and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

157. Plaintiff, on behalf of the Class, re-alleges and incorporates the above allegations as if fully set forth herein.

158. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' PII and PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII and PHI, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII and PHI; (2) to timely notify Plaintiff and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and do store.

159. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with its Plaintiff and Class Members, in particular, to keep secure their PII and PHI from disclosure without authorization from Plaintiff and the Class Members.

160. Defendant breached its fiduciary duty owed to Plaintiff and Class Members by failing to notify and/or warn Plaintiff and Class Members of the unauthorized disclosure of their PII and PHI.

161. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' PII and PHI from unauthorized disclosure.

162. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the compromise of their PII and PHI; and (ii) the diminished value of the services they received.

163. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V

Breach of Duty
(On Behalf of Plaintiff and the Class)

164. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

165. Defendants accepted the special confidence placed in them by Plaintiff and Class Members. There was an understanding between the parties that the Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of their PII and PHI.

166. Defendant became the guardian of Plaintiff's and Class Members' PII and PHI and accepted a fiduciary duty to act primarily for the benefit of Plaintiff and the Class Members, including safeguarding Plaintiff's and the Class Members' PII and PHI.

167. Defendant's fiduciary duty to act for the benefit of Plaintiff and Class Members pertains as well to matters within the scope of Defendant's duty to keep secure the Private Information of Plaintiff and the Class.

168. Defendants breached its fiduciary duty to Plaintiff and Class Members by (a) failing to protect their PII and PHI to Plaintiff and the Class; (b) by failing to notify Plaintiff and the Class Members of the unauthorized disclosure of the PII and PHI; and (c) by otherwise failing to safeguard Plaintiff's and the Class Members' PII and PHI.

169. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and/or Class Members have suffered and/or will suffer injury, including but not limited to: (a) the compromise of their PII and PHI; and (b) the diminished value of the services they received as a result of unauthorized exposing of Plaintiff's and Class Members' PII and PHI.

170. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI

Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

171. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

172. Defendants collected and maintained responsibility for the Private Information of Plaintiff and the Class, including, *inter alia*, name, Social Security Number, and other PHI in connection with the provision of services to Plaintiff and the Class.

173. At the time Defendants acquired the PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendants would safeguard the PII and not take unjustified risks when storing the PII.

174. Plaintiff and the Class would not have entrusted their PII to Defendants had they known that Defendants would fail to adequately safeguard their PII.

175. Prior to the Data Breach, Defendants published its HIPAA Notice, agreeing to protect and keep PHI of Plaintiff and the Class.

176. Implicit in the agreement between Plaintiff and Class Members and the Defendants to provide PII, was Defendant's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

177. In collecting and maintaining responsibility for the maintenance and protection of the PII of Plaintiff and the Class and publishing the Privacy Policy, Defendants entered into

contracts with Plaintiff and the Class requiring Defendants to protect and keep secure the PHI/PII of Plaintiff and the Class.

178. Plaintiff and the Class fully performed their obligations under the contracts with Defendants.

179. Defendants breached the contracts they made with Plaintiff and the Class by failing to protect and keep PHI/PII of Plaintiff and the Class.

180. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

181. As a direct and proximate result of Defendant's breach of contract, Plaintiff and the Class are at an increased risk of identity theft or fraud.

182. As a direct and proximate result of Defendant's breach of contract, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT VII
Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*
(On Behalf of Plaintiff and the Class)

183. Plaintiff, on behalf of herself and the Class, restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

184. Defendant is subject to the requirements of the CMIA, Cal. Civ. Code §56, *et seq.*

185. At all relevant times, Defendant maintained the PHI of Plaintiff and the Class for the "purpose of maintaining medical information to make the information available to the individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manager his or her information, or for the diagnosis or treatment of the individual."

186. Defendant is required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated and/or released without patient's authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

187. As a provider of health care or a contractor, Defendant is required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104.

188. Defendant is a person/entity licensed under California under California's Business and Professions Code, Division 2. See Cal. Bus. Prof. Code § 4000, *et seq.*

189. Plaintiff and Class Members had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network.

190. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Defendant's employees, which allowed the hackers to see and obtain Plaintiff's and Class Members' medical information.

191. Defendant negligently created, maintained, preserved, stored, and then exposed Plaintiff's and Class Members' individually identifiable "medical information," within the meaning of Cal. Civ. Code § 56.05(j), including Plaintiff's and Class members' names, addresses, medical information, and health insurance information, that alone or in combination with other publicly available information, reveals their identities. Specifically, Defendant knowingly allowed

and affirmatively acted in a manner that allowed unauthorized parties to access, exfiltrate, and actually view Plaintiff's and Class Members' confidential Private Information.

192. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff and Class Members to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and Class Members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

193. Defendant also violated Sections 56.06 and 56.101 of the CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential personal medical information.

194. Plaintiff's and Class Members' medical information was accessed and actually viewed by hackers in the Data Breach.

195. Plaintiff's and Class Members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

196. Defendant's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A). As a direct and proximate result of Defendant's above-noted wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia:

a. present, imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud –risks justifying expenditures for protective and remedial services for which they are entitled to compensation;

b. invasion of privacy;

c. breach of the confidentiality of the PHI;

d. statutory damages under the California CMIA;

e. deprivation of the value of their PHI, for which there is well-established national and international markets; and/or,

f. the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

197. As a direct and proximate result of Defendant's wrongful actions, inaction, omission, and want of ordinary care that directly and proximately caused the release of Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff's and Class Members' written authorization.

198. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and Class Members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA.

199. Plaintiff and the Class Members were injured and have suffered damages, as described above, from Defendant's illegal and unauthorized disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, which allows for actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

COUNT VIII
Invasion of Privacy
Cal. Const. Art. 1 § 1
(On Behalf of Plaintiff and the Class)

200. Plaintiff, on behalf of the Class, restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

201. Plaintiff brings this Count on her own behalf and on behalf of herself and the Class.

202. California established the right to privacy in Article I, Section 1 of the California Constitution.

203. Plaintiff and the Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

204. Defendant, headquartered in California and offering its services from California, owed a duty to its current and former patients, including Plaintiff and the Class, to keep their Private Information contained as a part thereof, confidential.

205. Defendant failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiff and the Class Members.

206. Defendant enabled and allowed unauthorized and unknown third parties access to and examination of the Private Information of Plaintiff and the Class Members, by way of Defendant's failure to protect the PII and PHI.

207. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and the Class Members is highly offensive to a reasonable person.

208. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class Members disclosed their Private Information to Defendant as part of their medical care or employment with Defendant, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure.

209. Plaintiff and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

210. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

211. Defendant acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that its information security practices were inadequate and insufficient.

212. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class Members.

213. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiff and the Class Members was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

214. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT IX
California Unfair Competition Law
Cal. Bus. & Prof. Code, § 17200, *et seq.*
(On Behalf of Plaintiff and the Class)

215. Plaintiff, on behalf of the Class, incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

216. Defendant is both organized under the laws of California and headquartered in California. Defendant violated California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code, § 17200, *et seq.*) by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard their PII and PHI from unauthorized disclosure, release, data breach, and theft; representing and advertising that they did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the Class' PII

and PHI; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class' PII and PHI;

b. by soliciting and collecting Class members' PII and PHI with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class Members' PII and PHI in an unsecure electronic environment;

c. by failing to disclose the Data Breach in a timely and accurate manner, in violation of California Civil Code section 1798.82;

d. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq.;*

e. by violating the CMIA, California Civil Code section 56, *et seq.*; and

f. by violating the CCRA, California Civil Code section 1798.82.

217. These unfair acts and practices were immortal, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq.*, CMIA, Cal. Civ. Code, § 56, *et seq.*, and the CCRA, Cal. Civ. Code, § 1798.81.5.

218. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff and the Class Members were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their PII and PHI, and additional losses described above.

219. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' PII and PHI and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-

named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

220. Plaintiff seeks relief under the UCL, including restitution to the Class of money or property that the Defendant may have acquired by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. Proc., § 1021.5), and injunctive or other equitable relief.

COUNT X
California Consumer Records Act
Cal. Civ. Code § 1798.82, *et seq.*
(On Behalf of Plaintiff and the Class)

221. Plaintiff, on behalf of the Class, incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

222. Defendant is both organized under the laws of California and headquartered in California. Defendant violated California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code, § 17200, *et seq.*) by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

g. by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard their PII and PHI from unauthorized disclosure, release, data breach, and theft; representing and advertising that they did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the Class' PII and PHI; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class' PII and PHI;

h. by soliciting and collecting Class members' PII and PHI with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class Members' PII and PHI in an unsecure electronic environment;

i. by failing to disclose the Data Breach in a timely and accurate manner, in violation of California Civil Code section 1798.82;

j. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq.;*

k. by violating the CMIA, California Civil Code section 56, *et seq.*; and

l. by violating the CCRA, California Civil Code section 1798.82.

223. These unfair acts and practices were immortal, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq.*, CMIA, Cal. Civ. Code, § 56, *et seq.*, and the CCRA, Cal. Civ. Code, § 1798.81.5.

224. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff and the Class Members were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their PII and PHI, and additional losses described above.

225. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' PII and PHI and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

226. Plaintiff seeks relief under the UCL, including restitution to the Class of money or property that the Defendant may have acquired by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. Proc., § 1021.5), and injunctive or other equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the proposed Class, prays for relief and judgment against Defendants as follows:

A. certifying the Class as defined herein pursuant to Section 382 of the Code of Civil Procedure, appointing Plaintiff as representatives of the Class, and designating Plaintiff's counsel as Class Counsel;

B. declaring that Defendant's conduct violates the laws referenced herein;

C. finding in favor of Plaintiff and the Class on all counts asserted herein;

D. awarding Plaintiff and the Class compensatory damages and actual damages in an amount to be determined by proof;

E. awarding Plaintiff and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiff and the Class punitive damages;

G. awarding Plaintiff and the Class civil penalties;

H. granting Plaintiff and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiff and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiff and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: February 26, 2024

Respectfully submitted,

BARRACK, RODOS & BACINE

By: /s/ Stephen R. Basser

STEPHEN R. BASSER (SBN 121590)
SAMUEL M. WARD (SBM 216562)
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874
sbasser@barrack.com
sward@barrack.com

EMERSON FIRM, PLLC
JOHN G. EMERSON*
2500 Wilcrest, Suite 300
Houston, TX 77042
Phone: 800-551-8649
Fax: 501-286-4659
jemerson@emersonfirm.com

Counsel for Plaintiff and the Putative Class
*Application for admission *Pro Hac Vice* to be filed