JULIAN HAMMOND (SBN 268489)
jhammond@hammondlawpc.com
POLINA BRANDLER (SBN 269086)
pbrandler@hammondlawpc.com
ARI CHERNIAK (SBN 290071)
acherniak@hammondlawpc.com
HAMMONDLAW, P.C.
11780 W Sample Rd., Suite 103
Coral Springs, FL 33065
(310) 601-6766
(310) 295-2385 (Fax)

Attorneys for Plaintiffs and the Putative Class

SUPERIOR COURT FOR THE STATE OF CALIFORNIA

COUNTY OF LOS ANGELES

JANE DOE 1 and **JANE DOE 2**, on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

PLANNED PARENTHOOD LOS ANGELES, a California Corporation,

Defendant.

CASE NO. 21STCV46178

CLASS ACTION COMPLAINT FOR:

(1) Violation of California Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq*.);
(2) Violation of California Customer Records Act (Cal. Civ. Code § 1798.80, *et seq*., § 1798.82);
(3) Violation of California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200, *et seq*.);
(4) Negligence; and
(5) Breach of Implied Contract

DEMAND FOR JURY TRIAL

Plaintiffs Jane Doe 1 and Jane Doe 2 ("Plaintiffs"), on behalf of themselves and all others similarly situated, by and through their attorneys of record, HammondLaw, P.C., complain and allege the following:

INTRODUCTION

1. This is a data breach class action brought on behalf of individuals whose private, sensitive personal identifiable information (PII) and private medical information (PMI), including patient names, dates of birth, addresses, insurance identification numbers, and clinical data, such as diagnosis, treatment, or prescription information, was exposed because of the failure of Planned Parenthood Los Angeles ("PPLA") to safeguard its healthcare consumers' privacy. As a result of PPLA's failure to maintain adequate data security, between approximately October 9, 2021 and October 17, 2021, a data breach occurred in which an unauthorized party or parties accessed PPLA's computer network, installed ransomware, and exfiltrated patient files. The PII and PMI of over 400,000 patients was compromised in the attack. Moreover, despite learning of the data breach on or about October 17, 2021, PPLA did not begin to notify affected individuals until November 30, 2021. The PII and PMI remains in the possession of the unauthorized party or parties.

2. PPLA's failure to adequately safeguard the PII and PMI of its patients and failure to timely notify them of the data breach placed those healthcare consumers at considerable risk of identity theft and fraud, causing the affected individuals to expend time, money, and resources addressing their damaged security interests and even their reputations. Plaintiffs and class members, as defined below, now face a significant risk of medical-related identity theft and fraud, financial fraud, and other identity-related fraud presently and into the indefinite future. This is particularly the case for the sensitive patient information kept by PPLA, which provides not only abortion and other family planning procedures, but also such health services as testing for sexually transmitted diseases, emergency contraception, and cancer screenings. Because PPLA provides these highly private services, and because PPLA is a lightning rod for public debate about abortion restrictions, the exfiltrated information is of the utmost sensitivity and subject to potential exploitation.

3. PPLA's significant delay in notifying affected healthcare consumers of the data breach underscores violation of PPLA's duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the compromised healthcare information, i.e., the PII and PMI of PPLA's patients.

4. Plaintiffs, on behalf of themselves and the class, seek injunctive and monetary relief to remedy the harm caused by PPLA's failure to adequately safeguard its patients' PII and PMI and PPLA's failure to timely notify them of the data breach.

PARTIES

5. Plaintiff Jane Doe 1 is an adult individual who resides, and at all relevant times, has resided in Los Angeles, California, and has obtained healthcare services from, has transacted business with, and has provided PII and PMI to PPLA.

6. Plaintiff Jane Doe 2 is an adult individual who resides, and at all relevant times, has resided in Los Angeles, California, and has obtained healthcare services from, has transacted business with, and has provided PII and PMI to PPLA.

7. Defendant PPLA is a California non-profit corporation with its principal office in Los Angeles, California.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action pursuant to California Code of Civil Procedure § 410.10. Some or all of the conduct and/or agreements that are subject of this dispute were made and deemed to have been entered into within California. The amount in controversy exceeds the jurisdictional minimum of this Court.

9. Venue is proper in this Court pursuant to California Code of Civil Procedure § 395. Defendant PPLA is headquartered in Los Angeles County, California and a substantial portion of the conduct giving rise to this action occurred within Los Angeles County.

FACTUAL ALLEGATIONS

10. PPLA operates approximately 20 healthcare facilities in and around Los Angeles, at which PPLA provides a panoply of health-related services, and particularly in the area of reproductive healthcare. On information and belief, PPLA has annual revenues of more than $90 million.

11. In the course of providing healthcare services at its facilities, PPLA requires healthcare consumers, as patients, to provide personal information including their full names, home address, dates of birth, Social Security numbers, financial information such as bank account and payment card numbers, and medical information including medical histories, past treatment and diagnostic records, prescription information, health provider information, and health insurance coverage. As a result, when patients are treated at a PPLA facility, their highly sensitive PII and PMI is obtained and maintained by PPLA on and through its computer systems for use by PPLA in providing healthcare services to its patients. During the course of providing healthcare services, PPLA further collects and maintains patient diagnostic, treatment, prescription, and insurance information on and through its computer systems.

12. Given the amount and sensitive nature of the data it collects, PPLA maintains a notice of "HIPAA Privacy Policy" on its website, which describes how PII and PMI about its patients will be used

and disclosed.[1] On information and belief, PPLA provides this Notice to all of its patients. The notice specifically states as follows: "We understand that health information about you and your health care is personal. We are committed to protecting health information about you." The notice further states: "Our pledge regarding your health information is backed-up by federal and state law. The privacy and security provisions of the federal Health Insurance Portability and Accountability Act ("HIPAA") require us to:

- Make sure that health information that identifies you is kept private;
- Make available this notice of our legal duties and privacy practices with respect to health information about you; and
- Follow the terms of the notice that is currently in effect."

13. Contrary to these representations, PPLA did not adequately maintain the security and confidentiality of the PII and PMI of its patients. As a result of PPLA's inadequate data security, between approximately October 9, 2021 and October 17, 2021, a data breach occurred in which an unauthorized party or parties accessed PPLA's computer network, installed ransomware, and exfiltrated patient files. The PII and PMI of over 400,000 patients was compromised in the attack. Moreover, despite learning of the data breach on or about October 17, 2021, PPLA did not begin to notify affected individuals until November 30, 2021. The PII and PMI remains in the possession of the unauthorized party or parties.

14. PPLA has represented to the United States Department of Health and Human Services Office for Civil Rights that 409,759 individuals have been affected by the foregoing data breach.[2]

15. Healthcare providers like PPLA are prime targets for data breaches because of the valuable PII and PMI that they collect and store for their healthcare consumers. The risk of hacking and unauthorized access to and disclosure of PII and PMI from healthcare providers was known to be prevalent at the time of the data breach. Indeed, in October 2020, the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA), along with the Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS), issued a Joint Cybersecurity Advisory entitled "Ransomware Activity Targeting the Healthcare and Public Health Sector."[3] This Advisory specifically warns that "CISA, FBI, and HHS have credible information of an increased and imminent

---

[1] *See* https://www.plannedparenthood.org/planned-parenthood-los-angeles/hipaa

[2] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (breach submission date November 30, 2021).

[3] *See* https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf.

cybercrime threat to U.S. hospitals and healthcare providers. CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats." The Advisory sets forth recommendations for cybersecurity best practices.

16. Despite such warnings of, and recommendations for mitigating, cybersecurity threats, however, PPLA failed to utilize data security best practices, failed to properly monitor its data storage vendor, and failed to take timely and reasonable precautions to protect the PII and PMI of its patients from unauthorized access and disclosure.

17. PPLA also failed to provide Plaintiffs and class members with reasonable, timely notice of the data breach. PPLA knew on or about October 17, 2021, that its computer systems had been hacked. PPLA did not begin to inform affected patients that their PII and PMI had been compromised until November 30, 2021. PPLA's failed to exercise diligence in promptly responding to the data breach. The delay is further symptomatic of PPLA's inadequate and unreasonable data security and further evidences violation of its duty to implement and maintain reasonable data security procedures and practices appropriate to the nature of the compromised information, i.e., identifiable personal and protected health information of PPLA's healthcare consumers.

18. PPLA's misconduct in failing to timely implement adequate and reasonable measures to protect Plaintiffs and class members' PII and PMI; failing to timely detect the data breach; failing to honor its promises, representations, and duties, including statutory duties, to protect Plaintiffs and class members' PII and PMI against unauthorized disclosure; and failure to provide timely and adequate notice of the data breach, caused substantial harm to Plaintiffs and class members in California.

19. Due to PPLA's negligence and data security failures, cyber criminals have obtained and now possess everything they need to commit personal and medical identity theft and wreak havoc on the financial and personal lives of over 400,000 individuals in California for decades to come. Plaintiffs and class members have already lost time and money responding to and mitigating the impact of the data breach and remain at continuing, ongoing, imminent, and impending risk of identity theft.

20. Plaintiffs relied upon PPLA's representations about the adequacy of its security policies and procedures to protect their PII and PMI; and would not have maintained their association with PPLA had they been made aware of PPLA's inadequate, deficient, and unreasonable data security.

21. PPLA has not provided affected individuals with identity protection services to protect against identity theft and fraud that could result at any time, over many years from the unauthorized disclosure of Plaintiffs and class members' PII and PMI. It can take years for identity theft victims to

even discover that they are the victim of medical-related identity theft or fraud. There can be a significant lag between when personal information is stolen and when it is misused for fraudulent purposes.

22. PPLA has failed to demonstrate or undertake appropriate and adequate measures to address the circumstances that caused the data breach or to prevent future occurrences.

Plaintiffs and Class Members Suffered Damages

23. The data breach announced by PPLA to its patients on or about November 30, 2021, was a direct and proximate result of PPLA's failure to properly safeguard and protect Plaintiffs and class members' PII and PMI from unauthorized access, use, and disclosure, as required by various state and federal statutes, regulations, industry practices, and the common law, including PPLA's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs and class members' PII and PMI to protect against reasonably foreseeable threats to the security or integrity of such information.

24. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting data breach, Plaintiffs and class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, changing the information used to verify their identity to information not subject to this data breach, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable. In addition, Plaintiffs and class members were subjected to continued and continuing risk of incurring unjustified expenses proximately resulting from the data breach including but not limited to purchasing extended credit monitoring and/or other remedial services to help minimize the risk of their PII and PMI being maliciously exposed and exploited, as well as expenses associated with unauthorized transactions resulting from malicious exposure and exploitation of their PII and PMI.

25. Defendant's wrongful actions and inaction directly and proximately caused the exfiltration, theft, and dissemination to unauthorized cybercriminals of Plaintiffs' and class members' PII and PMI, causing them to suffer, and to continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

(a) Identity theft and fraud resulting from the theft of their PII and/or PMI;

(b) Costs for credit monitoring, identity theft protection services, and other costs associated with the detection and prevention of identity theft and unauthorized use of their PII and/or PMI;

(c) Unauthorized use of their PII and/or PMI to commit medical insurance, social security, and/or financial fraud; unauthorized charges on their debit and credit card accounts; and the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII and PMI being placed in the hands of criminals and already misused via the sale of Plaintiffs and class members' PII and PMI on the Internet black market;

(d) Anxiety and emotional distress;

(e) Loss of privacy;

(f) Loss of the value of the explicit and implicit promises of data security;

(g) Untimely and inadequate notification of the data breach;

(h) Improper disclosure of patient medical information;

(i) Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

(j) Ascertainable losses in the form of deprivation of the value of their PII and PMI, for which there is a well-established national and international market;

(k) Loss of use of, control of, and/or access to their PII and/or PMI and costs associated with adverse effects on their credit including fraud and adverse credit notations; and

(l) Loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including medical and insurance fraud, social security fraud, finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, changing the information used to verify their identity to information not subject to this data breach, and the stress, nuisance, and annoyance of dealing with all such issues resulting from the data breach.

CLASS ACTION ALLEGATIONS

26. Plaintiffs bring this class action pursuant to Cal. Civ. Pro. Code. § 382 on behalf of themselves and the Class. The proposed Class (whose members are "Class Members") is defined as follows:

All residents of California whose PII or PMI was provided to or obtained by PPLA and whose PII or PMI was accessed, compromised, or stolen by an unauthorized individual or individuals in the data breach announced by PPLA on or about November 30, 2021.

27. Excluded from the Class are Defendant, Defendant's corporate parents, subsidiaries, affiliates, and any entity in which Defendant has a controlling interest; any of their officers, directors, employees, or agents; the legal representatives, successors, or assigns of any such excluded persons or entities; and the judicial officers to whom this matter is assigned as well as their court staff.

28. Numerosity. The members of the Class are so numerous that joinder of all members is impractical. PPLA has represented that 409,759 individuals were affected by the data breach. The precise number of Class Members, their identities, and their contact information can be ascertained through appropriate discovery and records of PPLA.

29. Commonality. Common questions of fact and law exist as to all members of the Class and predominate over the questions affecting only individual members of the Class. These common questions include but are not limited to:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Plaintiffs and Class Members' PII or PMI was accessed, compromised, or stolen in the data breach announced by PPLA;

c. Whether Defendant owed a duty to Plaintiffs and Class Members to implement and maintain reasonable security procedures and practices to adequately protect their PII and PMI;

d. Whether Defendant owed a duty to Plaintiffs and Class Members to provide them with timely and accurate notice of the data breach;

e. Whether Defendant breached its duties to protect the PII and PMI of Plaintiffs and the Class by failing to provide adequate data security;

f. Whether Defendant was negligent in the development, use, monitoring, or maintenance of data security protocols, failing to exercise a reasonable standard of care due in the circumstances;

g. Whether Defendant unreasonably delayed in notifying Plaintiffs and the Class of the data breach;

h. Whether Defendant was negligent in apprising affected individuals of the data breach;

i. Whether Defendant's conduct violated California statutory law;

j. Whether Defendant's breach of its duty to implement and maintain reasonable data security directly and/or proximately caused damages to Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to recover compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the data breach; and

l. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief and/or equitable relief.

30. Typicality. Plaintiffs' claims are typical of those of the Class because Plaintiffs and Class members were exposed to identical conduct and accompanying invasions of their privacy.

31. Adequacy. Plaintiffs can fairly and adequately represent the interests of the Class. Plaintiffs have no conflict of interest with other Class Members, are not subject to any unique defenses, and have retained competent and experienced counsel.

32. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because joinder of all members is impractical, the likelihood of individual members prosecuting separate claims is remote, and individual Class Members do not have a significant interest in controlling the prosecution of separate actions. Relief concerning Plaintiffs' rights under the laws alleged herein is appropriate with respect to the Class as a whole; and Plaintiffs anticipate no difficulty in the management of this action which would preclude its maintenance as a class action.

33. Plaintiffs reserve the right to add Class representatives, provided Defendant is afforded an opportunity to conduct discovery as to those representatives.

FIRST CAUSE OF ACTION
Violation of California's Confidentiality of Medical Information Act ("CMIA")
Cal. Civ. Code § 56, *et seq*.

34. Plaintiffs re-allege and incorporate by reference each and every allegation set forth in the preceding paragraphs.

35. Defendant is a "provider of healthcare" subject to the requirements of the CMIA.

36. Plaintiffs and Class Members are "patients" as defined in § 56.05 of the CMIA.

37. Plaintiffs and Class Members' PII and PMI constitutes "medical information" as defined in § 56.05(j) of the CMIA.

38. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs and Class Members' PII and PMI in a manner that preserved the confidentiality of the medical information contained therein violated the CMIA, Cal. Civ. Code § 56.101(a). Defendant's inadequate data security practices and protocols did not protect and preserve the confidentiality and integrity of electronic medical information in violation of the CMIA, Cal. Civ. Code § 56.101. As a result, Plaintiffs

and Class Members' PII and PMI were negligently released to unauthorized third parties who gained access to and possession of Plaintiffs and Class Members' PII and PMI.

39. Upon information and belief, the unauthorized cyber criminals gained access to the PII and PMI of Plaintiffs and Class Members with the intent of misusing this information, including marketing and selling this information on the dark web.

40. Plaintiffs and Class Members were injured and have suffered damages, as described above, from Defendant's negligent release of their medical information in violation of Cal. Civ. Code § 56.101, and therefore seek relief under Cal. Civ. Code § 56.36, including without limitation nominal damages of $1,000, actual damages, attorneys' fees, and costs.

41. Plaintiffs, on behalf of themselves and the Class, request relief as further described below.

SECOND CAUSE OF ACTION
Violation of California's Customer Records Act ("CRA")
California Civil Code § 1798.80 et seq.; § 1798.82

42. Plaintiffs re-allege and incorporate by reference each and every allegation set forth in the preceding paragraphs.

43. California Civil Code § 1798.82 provides that "(a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure shall be made *in the most expedient time possible and without unreasonable delay*, consistent with the legitimate needs of law enforcement . . . ." California Civil Code §1798.82(a) (Emphasis added).

44. Pursuant to California Civil Code § 1798.82(b), "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data *immediately following discovery*, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." California Civil Code § 1798.82(b) (Emphasis added).

45. Pursuant to California Civil Code § 1798.82(g) "breach of the security of the system" includes "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."

46. The CRA clearly defines the required standard of conduct relative to notice of a data breach involving personal information.

47. In enacting § 1798.82, the California Legislature noted that "[a]ccording to the Attorney General, victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative." 2002 Cal. Legis. Serv. Ch. 95 (SB 1386) at Section 1(e).

48. Under California Civil Code § 1798.80(a), "Business" means a "sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution." As a non-profit corporation, PPLA is a "business" within the meaning of § 1798.80(a).

49. "Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. California Civil Code § 1798.80(e).

50. Plaintiffs and Class Members are "customer[s]" within the meaning of the Civil Code § 1798.80(c) "who provide[d] personal information to [Defendant] for the purpose of . . . obtaining a service from the business." The PII and PMI retained by Defendant constitutes "personal information" as defined in Civil Code § 1798.80(e).

51. Defendant failed to provide timely notice required by California Civil Code § 1798.82(a) and/or (b) to Plaintiffs and the Class.

52. California Civil Code § 1798.82 was intended to prevent the type of harm that Defendant's failure to provide timely notice caused.

53. Plaintiffs and Class Members are California residents who provided personal information, including but not limited to PII and PMI, within the meaning of the CRA, to the Defendant. They are therefore members of the class of persons the statute was designed to protect.

54. Defendant's failure to comply with this statute proximately caused injury to Plaintiffs and the Class because Defendant did not notify Plaintiffs and the Class that their PII and PMI had been unlawfully accessed by unauthorized cybercriminals until more than six weeks after being apprised that a data breach had occurred.

55. If Plaintiffs and Class Members had been notified of the data breach earlier, they could have taken earlier steps to mitigate the dangers from their information being stolen. The unreasonable, six-week delay in notifying affected individuals after PPLA knew of the data breach harmfully exposed the PII and PMI of Plaintiffs and the Class to substantially increased risk of identity theft and fraud.

56. As a direct and proximate result of Defendant's unreasonable delay in notifying Plaintiffs and Class of the data breach, Plaintiffs and the Class have suffered and will continue to suffer damages as described above and continue to bear the risks of further exposure of their PII and PMI.

57. Plaintiffs, on behalf of themselves and the Class, seek relief pursuant to Cal. Civ. Code § 1798.84(b), requesting relief as described below.

THIRD CAUSE OF ACTION
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200 *et seq.*

58. Plaintiffs re-allege and incorporate by reference each and every allegation set forth in the preceding paragraphs.

59. Defendant has violated the California Unfair Competition Law, Business & Professions Code § 17200, et seq. ("UCL"), by engaging in unlawful, unfair and/or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL with respect to the services provided to the Class.

60. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs and Class Members' PII and PMI with knowledge that the information would not be adequately protected; and by negligently storing Plaintiffs and Class Members' PII and PMI in an unsecure electronic environment at least in violation of California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq*. as described above. Defendant also engaged in unlawful acts and practices by failing to disclose the data breach to Plaintiffs and Class Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82 as described above.

61. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiffs and Class Members were injured and lost, *inter alia*, money or property, including but not limited to the price received by Defendant for the services, the loss of Class Members' legally protected interest in the confidentiality and privacy of their PII and PMI, and nominal damages, as well as additional losses as described above.

62. Defendant knew or should have known that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and PMI and that the risk of a data breach or theft was likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of members of the Class.

63. Plaintiffs, on behalf of themselves and the Class Members, seek relief under the UCL including, but not limited to, restitution of money or property that Defendant may have acquired by means of its unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

64. Plaintiffs, on behalf of themselves and the Class, request relief as described below.

FOURTH CAUSE OF ACTION
Negligence

65. Plaintiffs re-allege and incorporate by reference each and every allegation set forth in the preceding paragraphs.

66. Defendant required Plaintiffs and Class Members to provide their PII and PMI as a condition of receiving healthcare services. Defendant collected and stored the data for purposes of providing healthcare services to Plaintiffs and Class Members.

67. Defendant owed Plaintiffs and Class Members a duty to exercise reasonable care in protecting their PII and PMI from unauthorized disclosure or access. Defendant acknowledged this duty in its Notice of Privacy Policy, where it promised not to disclose Plaintiffs and Class Members' PII and PMI.

68. Defendant owed Plaintiffs and Class Members a duty of care to provide security, consistent with industry standards, to ensure that Defendant's data security systems, procedures, and protocols adequately protected Plaintiffs' and Class Members' PII and PMI.

69. Defendant owed a duty to timely inform Plaintiffs and Class Members, in the event of a data breach, that their PII and PMI had been compromised or improperly disclosed to unauthorized third parties.

70. As a healthcare provider, Defendant had a special relationship with Plaintiffs and Class Members who entrusted Defendant with adequately protecting their PII and PMI.

71. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and PMI, Defendant's heightened targeting and vulnerability, as a healthcare provider, to data security attacks and breaches by cybercriminals.

72. Defendant breached its duties to Plaintiffs and Class Members in numerous ways, as described herein, including without limitation (a) failing to adequately protect Plaintiffs and Class Members' PII and PMI; (b) failing to maintain adequate data security practices to safeguard the PII and PMI; (c) failing to comply with healthcare industry standards for adequate data security; (d) failing to comply with its own privacy policies; (e) failing to comply with regulations protecting the PII and PMI at issue during the period of the data breach; (f) failing to adequately monitor, evaluate, and ensure the data security of Defendant's network, systems, and vendors; (g) failing to disclose the material fact that Defendant's data security practices were inadequate to safeguard the PII and PMI at issue; and (h) failing to disclose in a timely manner to Plaintiffs and Class Members the material fact of the data breach.

73. Plaintiffs' and Class Members' PII and PMI would not have been compromised but for Defendant's wrongful and negligent breach of its duties.

74. Defendant's failure to take proper security measures to protect the sensitive PII and PMI of Plaintiffs and Class Members as described in this Complaint created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of PII and PMI by unauthorized third parties. Given that healthcare providers are and at the time of the data breach were known to be prime targets for hackers, Plaintiffs and Class Members are part of a foreseeable, discernable group that was at high risk of having their PII and PMI compromised, misused, or otherwise wrongfully disclosed if not adequately protected by Defendant.

75. It was also foreseeable that Defendant's failure to provide timely and forthright notice of the data breach would result in injury to Plaintiffs and Class Members.

76. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered, and will continue to suffer, economic and non-economic harms as described above, including without limitation (a) costs associated with the continued and continuing exposure and unconsented disclosure of their PII and PMI to unauthorized third parties; (b) loss of value of their PII

and PMI; (c) out-of-pocket expenses associated with the prevention detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII and PMI; (d) lost time, effort, and opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recovery from fraud and identity theft; (e) lost time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (f) anxiety and emotional distress; (g) loss of privacy; (h) loss of fees paid to Defendant in reliance on its representations as to the veracity of its data security procedures and practices; and (i) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the continuing consequences of compromised PII and PMI for the foreseeable future.

77. Plaintiffs, on behalf of themselves and the Class, request relief as described below.

FIFTH CAUSE OF ACTION
Breach of Implied Contract

78. Plaintiffs re-allege and incorporate by reference each and every allegation set forth in the preceding paragraphs.

79. Plaintiffs and Class Members were required to provide their PII and PMI to Defendant in order to receive health care services and treatments.

80. As part of these transactions, Defendant agreed to safeguard and protect the PII and PMI of Plaintiffs and Class Members. Implicit in these transactions was the obligation that Defendant would use the PII and PMI for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

81. Additionally, Defendant implicitly promised to retain this PII and PMI only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the PII and PMI of Plaintiffs and Class Members from unauthorized disclosure or access.

82. Plaintiffs and Class Members entered into implied contracts with Defendant with the reasonable expectation that Defendant's data security practices and policies were adequate and consistent with healthcare industry standards. Plaintiffs and Class Members believed that Defendant would provide adequate and reasonable data security practices to protect their PII and PMI and would provide accurate and timely notice if such information was compromised, lost, or stolen.

83. Plaintiffs and Class Members would not have provided and entrusted their PII and PMI to Defendant in the absence of the implied contracts between them and Defendant whereby Defendant would

provide adequate and reasonable data security practices to protect their PII and PMI and would provide accurate and timely notice if such information was compromised, lost, or stolen.

84. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

85. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs and Class Members' PII and PMI, which was compromised as a result of the data breach, and by failing to time timely notify Plaintiffs and Class Members of the data breach.

86. As a direct and proximate result of Defendant's breaches of its implied contracts with Plaintiffs and Class Members, Plaintiffs and Class Members sustained actual losses and damages as described herein, and will continue to suffer damages for, potentially, years to come.

87. Plaintiffs, on behalf of themselves and the Class, request relief as described below.

PRAYER FOR RELEIEF

WHEREFORE, Plaintiffs Doe 1 and Doe 2, on behalf of themselves and members of the Class, respectfully request that this Court enter judgment in their favor and against Defendant as follows:

1. Certifying this matter as a Class action;

2. Awarding Plaintiffs and the Class all recoverable compensatory, consequential, actual and/or nominal/statutory damages in the maximum amount permitted by law;

3. Awarding other equitable relief;

4. Awarding appropriate injunctive relief;

5. Awarding attorneys' fees and costs as authorized by statute and governing law;

6. Awarding prejudgment interest at the legal rate; and

7. Granting such other and further relief, at law and in equity, as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and members of the Class, hereby demand a jury trial on all issues so triable pursuant to the California Rules of Civil Procedure.

DATED: December 20, 2021

Respectfully submitted,

Julian Hammond

Attorneys for Plaintiffs and the Putative Class