LAW OFFICES OF RONALD A. MARRON
RONALD A. MARRON (SBN 175650)
ron@consumersadvocates.com
ALEXIS WOOD (SBN 270200)
alexis@consumersadvocates.com
KAS L. GALLUCCI (SBN 288709)
kas@consumersadvocates.com
651 Arroyo Drive
San Diego, CA 92103
Telephone: (619) 696-9006
Facsimile: (619) 564-6665

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

JOHN DOE, a minor, by and through Guardian ad Litem, LATASHA POPE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

RADY CHILDREN'S HOSPITAL-SAN DIEGO, a California Corporation,

Defendant.

Case No.: **'21CV0114 JM RBB**

CLASS ACTION

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. California's Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56 *et seq.*
2. California Consumer Records Act
3. Negligence
4. Invasion of Privacy
5. Breach of Implied Contract

DEMAND FOR JURY TRIAL

Plaintiff John Doe ("Plaintiff"), a minor, by and through Guardian ad Litem, Latasha Pope, individually and on behalf of all others similarly situated, by and through undersigned counsel, hereby brings this Class Action against Rady Children's Hospital-San Diego ("Defendant") to, without limitation, obtain actual and exemplary damages, injunctive relief, restitution, and obtain a declaration that Defendant's actions were unlawful as further set forth below. Plaintiff alleges the following based upon personal knowledge as to himself and his own acts, and on information and belief as to all other matters, including, *inter alia*, any investigation conducted by and through his attorney.

NATURE OF THE ACTION

1. Defendant Rady Children's Hospital-San Diego is a regionally based hospital dedicated exclusively to pediatric health care. It is the largest children's hospital in California (based on admissions).

2. In or around the end of October 2020, Defendant announced a second data breach within this year involving the private medical information of approximately 19,788 of its patients disclosed to and viewed by an unauthorized party between February 7, 2020 and June 4, 2020. The medical information included highly valuable and protected information including patient names, addresses, dates of birth, the names of patients' physicians, and the department the patients were admitted to (Private Information).

3. Blackbaud, Inc., the company that provides the hospital fundraising and donor management software, allegedly notified Defendant of the breach at the end of 2020 despite announcing in May of 2020 that it had been the victim of a ransomware attack and data breach, exposing the private information and even private health information of its clients' students, patients, and donors.

4. Upon information and belief, once Blackbaud was aware of the cybercriminals, the company's IT experts expelled the hackers from the system, but

only after the hackers were able to remove a copy of a subset of Blackbaud's data. Blackbaud was then asked for compensation with the threat of releasing the data.

5. Plaintiff John Doe, through his Guardian ad Litem, Latasha Pope learned that his medical information was involved in the data breach after Ms. Pope received a notification letter from Defendant.

6. Plaintiff and the other Class Members' Private Information is now at risk because of Defendant's negligent conduct and unfair acts and practices. The Private Information that Defendant collected and maintained has been placed in the hands of criminal hackers. Defendant cannot reasonably maintain that the hackers destroyed the Private Information.

7. As a provider of health care, Defendant is subject to the requirements for preserving the confidentiality of medical information set forth under California's Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code §§ 56 *et seq.*

8. Defendant has a duty to reasonably protect the confidentiality of the medical information that it maintains, preserves, stores, abandons, destroys, or disposes of, and failure to comply with this duty exposes Defendant to liability for nominal and/or actual damages under Cal. Civ. Code § 56.36.

9. Defendant failed to uphold its duty under the CMIA when it allowed an unauthorized party to obtain the medical information of its patients.

10. Accordingly, Plaintiff brings this class action individually and on behalf of all others similarly situated and asserts the following causes of action: violations of the CMIA, California Consumer Records Act, negligence, invasion of privacy, and breach of implied contract.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), because at least one member of the Class, as defined below is a citizen of a different state than Defendant, there are more than 100 members of the

Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

12. The Court has personal jurisdiction over Defendant because Defendant's negligent acts or omissions and violations of consumer protection statutes regarding the security of Plaintiff's and Class Members' Private Information alleged herein caused injury to Plaintiff who is located in the Southern District of California.

13. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because the injury in this case substantially occurred in this District.

PARTIES

14. Plaintiff John Doe, a minor by and through Guardian Ad Litem, Latasha Pope, is a resident of San Diego County, California.

15. Defendant Rady Children's Hospital-San Diego, is a California non-profit corporation registered under entity number C0250564. Defendant's principal place of business is located at 3020 Children's Way, San Diego, California 92123.

FACTUAL ALLEGATIONS

Defendant's Obligations under the CMIA and Applicable Federal Law

16. Defendant is a regionalized pediatric center providing health care services within the County of San Diego.

17. Defendant is a provider of health care as defined under the California Confidentiality of Medical Information Act ("CMIA"). Cal. Civ. Code § 56.05(m).

18. As a provider of health care, Defendant must not disclose a patient's medical information without first obtaining an authorization. Cal. Civ. Code§ 56.10.

19. Further, every provider of health care who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information has a duty to preserve the confidentiality of the information contained therein. Cal. Civ. Code § 56.101(a).

20. "Any provider of health care . . . who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be

subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." Cal. Civ. Code § 56.101(a).

21. Defendant creates, maintains, preserves, stores, abandons, destroys, or disposes medical information. *See* **Exhibit 1**.

22. Defendant is thus required by the CMIA to take appropriate preventative actions to protect its patients' medical information against release consistent with Defendant's obligations under Civil Code § 56.36(e)(2)(E) and the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) (HIPAA) and all HIPAA Administrative Simplification Regulations in effect on January 1, 2012, contained in Parts 160, 162, and 164 of Title 45 of the Code of Federal Regulations, and Part 2 of Title 42 of the Code of Federal Regulations, including, but not limited to, all of the following:

i. Developing and implementing security policies and procedures.

ii. Designating a security official who is responsible for developing and implementing its security policies and procedures, including educating and training the workforce.

iii. Encrypting the information or records and protecting against the release or use of the encryption key and passwords, or transmitting the information or records in a manner designed to provide equal or greater protections against improper disclosures.

The Data Breach

23. On October 29, 2020, Defendant issued a press release on its website stating that it "recently learned that one of its third-party service providers, Blackbaud," had experienced a data breach involving "information about members of the Rady Children's Hospital-San Diego community" (hereinafter referred to as the "Data Breach"). *See* **Exhibit 2.**

24. The press release went on to state that between February 7, 2020 and June 4, 2020, "an unauthorized party had access to backup files for the Blackbaud fundraising software." *See id.*

25. Blackbaud supplies fundraising and donor management software to the Defendant.

26. Defendant uses and shares certain information from its patients to contact said patients or the parents/guardians of its patients in connection with Defendant's fundraising activities. This information includes patients' names, address, age, gender, date of birth, telephone number, and other contact information (such as email address), dates of when patients received care at Rady Children's, the name of their treating physician, their general department of service, and health insurance status. *See* **Exhibit 1.**

27. The information Defendant uses and shares in connection with its fundraising activities is protected medical information as defined under Cal. Civ. Code § 56.05(j).

28. Defendant claimed it determined the Personal Information for members of its community was contained in the backup files on October 7, 2020. The personal information involved names, addresses, physician, date of admission, department of service, and date of birth. *See* **Exhibit 2.**

29. Due to the breach, Plaintiff and Class Members' Private Information was viewed by the unauthorized hacker.

30. The Personal Information involved in the Data Breach is protected medical information as defined under Cal. Civ. Code § 56.05(j).

31. Defendant further stated in its press release that "Blackbaud has represented that they are monitoring the dark web for any exchange of personal information related to this incident." *See* **Exhibit 2**.

32. However, the press release fails to mention that the attack on Blackbaud's security system involved the donor information from hundreds of

nonprofits and institutions. *See* Doug Kreitzberg, *Blackbaud Breach Leaves Hundreds of Non-Profits Scrambling*, Designed Privacy, July 31, 2020, https://designedprivacy.com/blackbaud-breach/#:~:text=The%20Blackbaud%20breach%20is%20just%20the%20latest%20reminder,hackers%20stole%20a%20copy%20of%20a%20data%20set (last visited November 25, 2020).

33. On information and belief, Blackbaud has not provided verification or further details regarding the disposition of the data to confirm that the stolen data has been destroyed. Nor does Defendant or Blackbaud know whether the hackers maintained the data in a sufficiently secure manner to prevent others from acquiring the Private Information.

34. On information and belief, Plaintiff's and the other Class Members' Private Information was copied multiple times by unauthorized users, not destroyed, and the data has been or may be sold and misused at a later date.

35. On October 29, 2020, Defendant reported the Data Breach to the California State Attorney General. Defendant additionally submitted a breach notification sample of a letter entitled "Notice of Data Security Incident" wherein it outlines the information set forth in its press release in addition to offering complimentary identity monitoring services for an unspecified amount of time. *See* **Exhibit 3.**

36. In reporting the Data Breach to the Attorney General, Defendant effectively admits that the Data Breach involved a "breach of [its] security system." *See* Cal. Civ. Code § 1798.82(f).

37. A "breach of the security of the system" is defined as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." Cal. Civ. Code § 1798.82(g).

38. Accordingly, the Data Breach compromised the security, confidentiality, or integrity of the medical information involved in the breach.

39. On October 30, 2020, Defendant also reported the breach to the Secretary of the U.S. Department of Health and Human Services Office for Civil Rights. Defendant reported that the breach affected approximately 19,788 individuals. *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited January 20, 2021).

40. In reporting the Data Breach to the Secretary of the U.S. Department of Health and Human Services Office for Civil Rights, Defendant effectively admits that the medical information involved in the Data Breach was unsecured protected health information as defined by 45 C.F.R. § 164.402. *See* 45 C.F.R. § 164.408.

41. Unsecured protected health information is defined 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 Secretary." 45 C.F.R. § 164.402.

42. This is not the first time Defendant has failed to reasonably protect and preserve the confidentiality of medical information of its patients. Defendant was previously investigated by the California Department of Public Health for a four separate reported disclosures of unencrypted patient data of 20,421 of its patients between June 16, 2014 and July 25, 2015. Following an investigation of the incident, the California Department of Public Health found Defendant "failed to prevent unlawful or unauthorized access to, or use or disclosure of, patients' medical information in violation of Health and Safety Code Section 1280.15, subdivision (a)." Rady Children's Hospital – San Diego Statement of Deficiencies and Plan of Correction, December 1, 2015 https://www.cdph.ca.gov/Programs/CHCQ/LCP/CDPH%20Document%20Library/Breaches/RadyChildrensHospitalAPBreach_080011817.pdf (last visited January 20, 2021).

43. As a result, the California Department of Public Health fined Defendant penalties of up to $25,000 per patient whose medical information was disclosed. *See* Penalties Issued in 2016, California Department of Public Health, https://www.cdph.ca.gov/Programs/CHCQ/LCP/Pages/MedicalBreaches.aspx (last visited January 20, 2021) (lists Rady Children's Hospital - San Diego); *see also* Rady Children's Hospital – San Diego Statement of Deficiencies and Plan of Correction, December 1, 2015 https://www.cdph.ca.gov/Programs/CHCQ/LCP/CDPH%20Document%20Library/Breaches/RadyChildrensHospitalAPBreach_080011817.pdf ("The department, after investigation, may assess an administrative penalty for a violation of [Health & Safety Code § 1280.15(a)] may assess an administrative penalty of up to twenty-five thousand dollars ($25,000) per patient whose medical information was unlawfully or without authorization accessed, used, or disclosed.")

44. As recently as February 21, 2020, another data breach involving the Defendant was reported to the California Attorney General. Defendant reported a data security incident involving the radiology-related information of 2,360 patients occurred between the dates of June 20, 2019 and January 5, 2020. A class action was filed on July 1, 2020 by Jose Orozco under case no. 37-2020-00023102-CU-NP-CTL in San Diego Superior Court. *Orozco v. Rady Children's Hospital-San Diego*, No. 37-2020-00023102-CU-NP-CTL, Register of Actions 1, Plaintiff's Class Action Complaint, San Diego Superior Court.

45. The latest data breach involving approximately 19,788 individuals' private medical information surpasses both of the prior data breaches, combined, and is further evidence that Defendant's conduct and practices as it relates to the preserving the confidentiality of its patients' medical information failed to reasonably protect said information from unauthorized disclosure in violation of Cal. Civ. Code 56.101(a).

46. Defendant had the resources necessary to protect and preserve confidentiality of electronic medical information of Plaintiff and the Class in its possession, but neglected to adequately implement data security measures according to its representations to Plaintiff and the Class and as required by the Act, despite its obligation to do so. Additionally, the risk of vulnerabilities in its computer and data systems of being exploited by an unauthorized third party trying to steal Plaintiff's and the Class' medical information was foreseeable and/or known to Defendant.

47. "Healthcare organization[s] need to ensure that their systems are well protected against cyberattacks, which means investing in technologies to secure the network perimeter, detect intrusions, and block malware and phishing threats." *See Cybersecurity Best Practices for Healthcare Organizations*, HIPAA Journal, Nov. 1, 2018, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (lasted visited January 20, 2021).

Defendant Expressly Promised to Protect Its Patients' Medical Information

48. Defendant's privacy policy states it is "committed to protecting the privacy of medical information" and that it has "a duty and responsibility to safeguard patient medical information." *See* **Exhibit 1** at pg. 4, PURPOSE OF THIS NOTICE.

49. Notwithstanding the foregoing promises, Defendant failed to protect the medical information of the patients' whose information was involved in the Data Breach, as conceded in Defendant's notification letters.

50. If Defendant truly understood the importance of safeguarding its patients' medical information, it would acknowledge its responsibility for the harm it has caused, and would compensate them, provide long-term protection, agree to Court-ordered and enforceable changes to its cybersecurity policies and procedures, and adopt regular and intensive training to ensure that a data breach like this never happens again.

51. Defendant's data security obligations were particularly important given the known substantial increase in data breaches in the healthcare industry, including the recent data breaches involving the Defendant itself.

Facts Specific to Plaintiff

52. Plaintiff, like each member of the proposed Class, was admitted as a patient for treatment and services at one of Defendant's locations.

53. Plaintiff, like each member of the proposed Class, provided Defendant with individually identifiable medical information as defined under Cal. Civ. Code § 56.05(j) when they received medical services from Defendant.

54. Plaintiff, like each member of the proposed Class, expected Defendant to maintain the privacy of their medical information as set forth under its privacy practices and state and federal law.

55. Defendant sent Latasha Pope, guardian of Plaintiff, a letter entitled "Notice of Data Security Incident" and signed by Christina Galbo, MBA, CHC, Chief Compliance and Privacy Officer, admitting and confirming that his personal medical information in Defendant's possession had been stolen.

56. Apart from offering complimentary identity monitoring services, Defendant does nothing to mitigate the harms caused by the Data Breach.

57. Defendant's offer of identity monitoring services is woefully inadequate. When it comes to identity theft, there is often time a lag between when harm occurs versus when it is discovered, and also between when medical information is acquired and when it is used. Furthermore, identity monitoring services only alert someone to the fact that they have already been the victim of identity theft, they do *not* prevent identity theft. *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited January 20, 2021).

58. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, substantial and continuing

increased risk of harm from fraud and identity theft. Plaintiff and Class Members must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

59. This risk is made even more concerning by the fact that members of the Class, including the Plaintiff, are minors and thus stand to lose more than what is at usually at stake with identity theft given their lack of credit history and the fact that their information can be used to create a "clean slate identity."

60. Child identity theft has become more prevalent over the years in large part because the crime is more difficult to detect. "When an unauthorized person uses your credit card number to make unauthorized purchases, most banks will contact you the moment they suspect suspicious activity. But when an unauthorized person uses your child's name successfully to get a credit card—either by using a pre-approved card offer stolen from a mailbox or by creating a synthetic identity and applying for a new card—it is highly unlikely that anyone will contact you. As far as the bank or credit bureau is concerned, the false identity is real because thieves use a child's clean slate to establish a new credit history." *See* Brett Singer, *What Is Child Identity Theft?*, Apr. 13, 2014, https://www.parents.com/kids/safety/tips/what-is-child-identity-theft/ (last visited January 20, 2021).

61. Identity theft "can wreak havoc on [] children's credit and even leave them with a massive debt before they've even reached voting age." In 2017, alone, more than one million children were the victims of identity fraud. *See* Casey Bond, *How to Check Your Child's Credit Report*, Feb. 5, 2019, https://creditcards.usnews.com/articles/how-to-check-your-childs-credit-report#:~:text=%20Protecting%20Your%20Child%27s%20Credit%20%201%20Kee

p,that%20contain%20your%20child%27s%20sensitive%20personal...%20More%20 (last visited January 20, 2021).

62. Plaintiff and the Class Members have suffered, continue to suffer and/or will suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal medical information;

b. Improper disclosure of their medical information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their medical information being placed in the hands of criminals;

d. The imminent and certainly impending risk of having their medical information used against them by spam callers to defraud them;

e. Loss of privacy suffered as a result of the Data Breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

g. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' personal identifiable information within their medical information, for which there is a well-established and quantifiable national and international market;

h. Damage to their credit due to fraudulent use of their medical information; and

i. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

63. Moreover, Plaintiff and Class Members have an interest in ensuring that their medical information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

64. Defendant itself acknowledged the harm caused by the Data Breach by offering Plaintiff and Class Members' identity theft monitoring services. However,

the identity theft monitoring is woefully inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk and does nothing to reimburse Plaintiff and Class Members for the injuries they have already suffered.

CLASS ACTION ALLEGATIONS

65. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of himself and a nationwide Class defined as follows:

> **National Class**: All persons in the United States whose Private Information was compromised as a result of the Data Breach announced by Defendant on or around October 29, 2020.
>
> **California Sub-Class**: All persons in California whose Private Information was compromised as a result of the Data Breach announced by Defendant on or around October 29, 2020.

66. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which the Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of such excluded persons.

67. Numerosity. The members in the proposed Class are approximately 19,788 individuals. Accordingly, individual joinder of all members is impracticable, and the disposition of the claims of all Class Members in a single action will provide substantial benefits to the parties and Court.

68. Commonality. Questions of law and fact common to Plaintiffs and the Class include:

a. Whether Defendant violated the laws asserted herein, including without limitation the California Confidentiality of Medical Information Act,

Cal. Civ. Code §§ 56 *et seq* and the Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.*

b. Whether Defendant had a duty to use reasonable care to safeguard Plaintiff and the Class Members' medical information.

c. Whether Defendant breached its contractual promises to safeguard Plaintiff and the Class Members' medical information.

d. Whether Defendant knew or should have known about the inadequacies of their date security polices and system and the dangers associated with storing sensitive medical information.

e. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and the other Class Members' medical information from unauthorized release and disclosure.

f. Whether Defendant's conduct was deceptive, unfair, unconscionable, or constituted unfair competition.

g. Whether Defendant's conduct was likely to deceive a reasonable consumer.

h. Whether Defendant is liable for negligence or gross negligence.

i. Whether Plaintiff and the Class are entitled to nominal damages, actual damages.

j. Whether Defendant's conduct in regard to the Data Breach violated applicable state laws.

k. Whether Plaintiff and Class were injured as a proximate cause or result of the Data Breach.

l. Whether Defendant's practices and representations related to the Data Breach breached implied warranties.

m. Whether Defendant has been unjustly enriched as a result of the conduct complained of herein.

n. Whether Plaintiff and the Class are entitled to damages, restitutionary, injunctive, declaratory, or other relief.

69. Typicality. Plaintiff is a member of the Class. Plaintiff's claims are typical of the claims of each Class member in that Plaintiff and Class Members sustained damages arising out of Defendant's Data Breach, wrongful conduct and unlawful practices, and Plaintiff and Class Members sustained similar injuries and damages as a result of Defendant's uniform illegal conduct.

70. Adequacy. Plaintiff is an adequate class representative because Plaintiff's interests do not conflict with the interests of the Class he seeks to represent. Plaintiff's claims are common to all members of the Class, and Plaintiff has a strong interest in vindicating the rights of absent Class Members. Plaintiff has retained counsel competent and experienced in complex class action litigation, and they intend to vigorously prosecute this action.

71. Ascertainability. Class Members can easily be identified by the objective criteria set forth in the Class definition.

72. Predominance. The common issues of law and fact identified above predominate over any other questions affecting only individual members of the Class. Class issues fully predominate over any individual issue.

73. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because: (a) the joinder of all individual Class Members is impracticable, cumbersome, unduly burdensome, and a waste of judicial and/or litigation resources; (b) the individual claims of the Class Members may be relatively modest compared with the expense of litigating the claim, thereby making it impracticable, unduly burdensome, and expensive to justify individual actions; (c) when Defendant's liability has been adjudicated, all Class Members' claims can be determined by the Court and administered efficiently in a manner far less burdensome and expensive than if it were attempted through filing, discovery, and trial of all individual cases.

74. This class action is properly brought and should be maintained as a class action because questions of law or fact common to Class Members predominate over any questions affecting only individual members, and because a class action is superior to other available methods for fairly and efficiently adjudicating this controversy.

75. This class action is also properly brought and should be maintained as a class action because Plaintiff seeks injunctive relief on behalf of the Class Members on grounds generally applicable to the Class. Certification is appropriate because Defendant has acted or refused to act in a manner that applies generally to the injunctive Class (i.e., Defendant has failed to reasonably protect Plaintiff and the Class Members' medical information). Thus, any final injunctive relief or declaratory relief would benefit the Class as a whole.

COUNT ONE

Violations of the CMIA

76. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

77. Plaintiff brings this claim individually and on behalf of all Classes, or in the alternative, the California Sub-Class.

78. Defendant is a "provider of health care" as defined under Cal. Civ. Code § 56.05(m).

79. Defendant created, maintained, preserved, and stored Plaintiff and the Class' "medical information" as defined under Cal. Civ. Code 56.05(j) which was subject to the Data Breach.

80. Plaintiff and Class Members are "Patients" as defined by Cal. Civ. Code § 56.05(k).

81. As a provider of health care, Defendant owed a duty to preserve the confidentiality of Plaintiff's and the Class' medical information and to not allow Plaintiff and the Class' medical information to be release and viewed by unauthorized

persons. Defendant breached its duty owed to Plaintiff and the Class by failing to utilize a vendor with fair, reasonable, or adequate computer systems and data security policies to safeguard Plaintiff's and Class Members' medical information and allowing that Private Information to be released and viewed by unauthorized persons.

82. In violation of Cal. Civ. Code § 56.10(a), Defendant disclosed Plaintiff's and the Class Members' Private Information (including medical information) without first obtaining an authorization. The unauthorized disclosure of Plaintiff's and the Class Members' Private Information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Defendant who knew or should have known that its vendor had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known of the risks inherent in collecting and storing the protected medical information of Plaintiff and the Class. This release of Plaintiff's and Class Members' Private Information to unauthorized hackers during the Data Breach was an affirmative act in violation of violation of Cal. Civ. Code § 56.10(a). Plaintiff's and the Class Members' Private Information was viewed by the unauthorized hackers as a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56.10(a).

83. In violation of the first sentence of Cal. Civ. Code § 65.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information (including Plaintiff's and the Class Members' Private Information (including medical information) in a manner that failed to preserve and breached the confidentiality of the information contained therein. This violation resulted from the affirmative actions of Defendant who knew or should have known that its vendor had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known of the risks inherent in collecting and storing the protected medical information of Plaintiff and the Class. This release of Plaintiff's and Class Members' Private Information to unauthorized hackers during the Data Breach was an affirmative communicative act

in violation of violation of Cal. Civ. Code § 56.101(a). Plaintiff's and the Class Members' Private Information was viewed by the unauthorized hackers as a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56.101(a).

84. In violation of the second sentence of Cal. Civ. Code § 56.101(a), Defendant negligently Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information (including Plaintiff's and the Class Members' Private Information (including medical information). This violation resulted from the affirmative actions of Defendant who knew or should have known that its vendor had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known of the risks inherent in collecting and storing the protected medical information of Plaintiff and the Class. This release of Plaintiff's and Class Members' Private Information to unauthorized hackers during the Data Breach was an affirmative communicative act in violation of violation of Cal. Civ. Code § 56.101(a). Plaintiff's and the Class Members' Private Information was viewed by the unauthorized hackers as a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56.101(a).

85. The Plaintiff's and the Class Members' Private Information that was subject to the Data Breach included "electronic medical records" or "electronic health records" as referenced by Cal. Civ. Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

86. In violation of Cal. Civ. Code § 56.101(b)(1)(A), Defendant's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information (including Plaintiff's and Class Members' Private Information). This violation resulted from the affirmative actions of Defendant who knew or should have known that its vendor had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known of the risks inherent in collecting and storing the protected medical information of Plaintiff and the Class. This release of

Plaintiff's and Class Members' Private Information to unauthorized hackers during the Data Breach was an affirmative communicative act in violation of violation of Cal. Civ. Code § 56.101(b)(1)(A). Plaintiff's and the Class Members Private Information was viewed by the unauthorized hackers as a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56.101(b)(1)(A).

87. In violation of Cal. Civ. Code § 56.101(b)(1)(B), Defendant's electronic health record system or electronic medical record system failed to automatically record and preserve any change or deletion of any electronically stored medical information (including Plaintiff's and Class Members' Private Information). This violation resulted from the affirmative actions of Defendant who knew or should have known that its vendor had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known of the risks inherent in collecting and storing the protected medical information of Plaintiff and the Class.

88. In violation of Cal. Civ. Code § 56.101(b)(1)(B), Defendant's electronic health record system or electronic medical record system failed to record the identity of persons who accessed and changed medical information (including Plaintiff's and the Class Member's Private Information), failed to record the date and time medical information was accessed (including Plaintiff's and the Class Member's Private Information), and failed to record changes that were made to medical information (including Plaintiff's and the Class Members' Private Information). This violation resulted from the affirmative actions of Defendant who knew or should have known that its vendor had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known of the risks inherent in collecting and storing the protected medical information of Plaintiff and the Class.

89. In violation of Cal. Civ. Code § 56.36(b) Defendant negligently released confidential information or records concerning Plaintiff's and Class Members'

(including Plaintiff's and Class Members' Private Information). This negligent release of Plaintiff's and Class Members' Private Information to unauthorized hackers during the Data Breach was an affirmative communicative act in violation of Cal. Civ. Code § 56.36(b). Plaintiff's and the Class Members' Private Information was viewed by the unauthorized hackers as a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56.36(b).

90. In violation of Cal. Civ. Code § 56.10(e), Defendant disclosed Plaintiff's and Class Members' Private Information to persons or entities not engaged in providing direct health care services to Plaintiff or Class Members or their providers of health care or health care service plans or insurers or self-insured employers. This violation resulted from the affirmative actions of Defendant who knew or should have known that its vendor had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known of the risks inherent in collecting and storing the protected medical information of Plaintiff and the Class.

91. The injury and harm suffered by Plaintiff and the Class was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and its breach would cause Plaintiff and the Class to suffer the foreseeable harms associated with the exposure of their medical information.

92. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class now face an increased risk of future harm.

93. Pursuant to Cal. Civ. Code §§ 56.35 and 56.36, Plaintiff and each member of the Class seek relief including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses and costs. A recovery of nominal damages does not require that the plaintiff have suffered or have been threatened with actual damages.

94. As a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56 *et seq.*, Plaintiff and Class Members now face an increased risk of future harm.

95. As a direct and proximate result of Defendant's violation of Cal. Civ. Code § 56 *et seq.*, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

96. Plaintiff and Class Members suffered a privacy injury by having their sensitive medical information disclosed, irrespective of whether or not they subsequently suffered identity fraud or incurred any mitigation damages. Medical information has been recognized a private sensitive information in common law and federal and state statutory schemes and the disclosure of such information resulted in cognizable injury to Plaintiff and Class Members.

COUNT TWO

California Consumer Records Act

97. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

98. Plaintiff brings this claim individually and on behalf of all Classes, or in the alternative, the California Sub-Class.

99. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "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 whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person," Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonably delay…"

100. The CCRA further provides: "Any 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 any 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." Cal. Civ. Code § 1798.82(b).

101. Any person or business that is required to issue a security breach notification under the CCRA shall meet all the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

iii. If the information is possible to determine at the time the notice is provided, then any of the follow:

1. The date of the breach;
2. The estimated date of the breach; or
3. The date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

vi. The toll-free telephone number and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

102. The Data Breach described herein constituted a "breach of the security system" of Defendant.

103. Blackbaud announced in May of 2020 that it had been the victim of a ransomware attack and data breach, exposing the private information and even private health information of its clients' students, patients, and donors. However, Defendant did not inform Plaintiff and Class Members about the Data Breach, affecting their Private Information, under the end of October of 2020.

104. Defendant failed to disclose to Plaintiff and Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Private Information, when Defendant knew or reasonably believed such information had been compromised.

105. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

106. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff and Class Members would impede its investigation.

107. As a result of Defendant's violation of Cal. Civ. Code § 1798.82(b), Plaintiff and Class Members were deprived of prompt notice of the Data Brach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection. These measures could have prevented some of the damages suffered by Plaintiff and Class Members because their Private Information would have had less value to identity thieves.

108. As a result of Defendant's violation Cal. Civ. Code § 1798.82(b), Plaintiff and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

109. Plaintiff and Class Member seek all remedies available under Cal. Civ. Code § 1798.82(b), including but not limited to the damages suffered by Plaintiff and Class Members as alleged above and equitable relief.

110. Defendant's misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiff and Class Members of "legal rights or otherwise causing injury." In addition, Defendant's misconduct as alleged herein is malice or oppression under Cal. Civ. Code § 3294(c)(1) and (c) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff and Class Members and despicable conduct that has subjected Plaintiff and Class Members to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiff and Class Members are entitled to punitive damages against Defendant under Cal. Civ. Code § 3294(a).

COUNT THREE

Negligence

111. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

112. Plaintiff brings this claim individually and on behalf of all the Classes.

113. Plaintiff and Class Members entrusted their medical information to Defendant. Defendant owed to Plaintiff and the other Class Members a duty to exercise reasonable care in handling and using their medical information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the data breaches, theft, and unauthorized use, and to promptly detect attempts at unauthorized access.

114. Defendant owed a duty of care to Plaintiff and Class Members because Plaintiff and Class Members were foreseeable and probable victims of Defendant's failure to secure their medical information. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' medical information by disclosing and providing access to this information

to unauthorized third parties and by failing to properly supervise the manner in which the medical information was stored, used, and exchanged.

115. Defendant had a "special relationship" with Plaintiff and Class Members. The willingness to share and entrust Plaintiff and Class Member's Private Information with Defendant as predicated on the understanding that Defendant would take adequate security precautions.

116. The risk that unauthorized persons would attempt to gain access to the medical information and misuse was foreseeable. As the holder of vast amounts of medical information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the medical information.

117. Such information is highly valuable, and Defendant is aware of other instances when criminals have attempted to access, and in fact have accessed medical information from Defendant, its affiliates, and others. Defendant has been targeted by criminals successfully in the past by such attempts. Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the medical information of Plaintiff and the other Class Members, and the importance of exercising reasonable care in handling it.

118. Defendant breached its duty by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and medical information of Plaintiff and the other Class Members which actually and proximately caused the Data Breach and Plaintiff's and the other Class Members' injuries. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages.

119. Defendant's breach of its common law duties to exercise reasonable care and it's failures and negligence actually and proximately caused the Plaintiff and other Class Members actual, tangible injury-in-fact, and damages, including without limitation the theft of their medical information by criminals, improper disclosure of

their medical information, lost value of their personal information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted and was caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT FOUR

Invasion of Privacy and Violation of the California Constitution, Art. 1, § 1

120. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

121. Plaintiff brings this claim individually and on behalf of all the Classes.

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

123. The State of California recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts which states: One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. Restatement (Second) of Torts § 652B (1977).

124. Plaintiff and Class Members had a legitimate and reasonable expectation of privacy with respect to their medical information and were accordingly entitled to the protection of this information against disclosure to and acquisition by unauthorized third parties.

125. Defendant published private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and Class Members by disclosing and exposing Plaintiff's and Class Members' medical information to an unauthorized third-party through its negligent security practices, thereby making it reasonably likely that such information will become known to the public, including without limitation on the dark web and elsewhere.

126. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their medical information to Defendant as part of their use of Defendant's services, but privately, with the intention that the medical information would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

127. The Data Breach constitutes an intentional interference with Plaintiff's and Class Members' 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.

128. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

129. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

130. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' medical information was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

131. 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 Class Members in that the medical information maintained by Defendant can be accessed, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized persons.

132. Plaintiff and Class Members have no adequate remedy at law for these injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT FIVE

Breach of Implied Contract

133. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

134. Plaintiff brings this claim individually and on behalf of all the Classes.

135. When Plaintiff and the Class Members provided their medical information to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect their medical information.

136. Based on the implicit understanding, Plaintiff and Class Members accepted Defendant's offers of health services and provided Defendant with their medical information.

137. Plaintiff and Class Members would not have provided their medical information to Defendant had they known that Defendant would not safeguard their medical information as promised.

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

139. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' medical information.

140. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of the implied contract with Plaintiff and Class Members.

PRAYER FOR RELIEF

141. Wherefore, Plaintiff, individually and on behalf of all others similarly situated, prays for judgment against Defendant as to each and every cause of action, and the following remedies:

a. An Order declaring this action to be a proper class action, appointing Plaintiff as class representatives, and appointing their undersigned counsel as class counsel;

b. An Order awarding Plaintiff and Class Members appropriate monetary relief, including actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution and disgorgement;

c. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

d. An award of attorneys' fees and costs, as allowed by law; and

e. Any other or further relief as may be appropriate under the circumstances.

JURY DEMAND

142. Plaintiff hereby demands a trial by jury on all issues so triable.

Date: January 20, 2021

LAW OFFICES OF RONALD A. MARRON

By: */s/ Ronald A. Marron*

RONALD A. MARRON
ALEXIS M. WOOD
KAS L. GALLUCCI
651 Arroyo Drive
San Diego, California 92103
Telephone: (619) 696-9006
Facsimile: (619) 564-6665