BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ltfisher@bursor.com

Attorney for Plaintiff

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES

MICHELLE GARZA, individually and on behalf of all others similarly situated,

Plaintiff,

v.

PLANNED PARENTHOOD LOS ANGELES,

Defendant.

Case No. 21STCV47357

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Michelle Garza ("Plaintiff") brings this action on behalf of herself and all others similarly situated against Planned Parenthood Los Angeles ("PPLA" or "Defendant"), alleging as follows based upon information, belief and investigation of counsel, except as to the allegations specifically pertaining to her, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action arising from Defendant's failure to safeguard personally identifying information ("PII") and personal health information ("PHI") of over 400,000 patients entrusted to it in its role as a health care provider. Specifically, this action arises from Defendant's reliance on an outdated and insecure information storage system that proved readily penetrable to nefarious hackers in October 2021, resulting in the exposure of sensitive information, such as health insurance details, names, dates of birth, addresses, telephone numbers, email addresses, and clinical data.

2. PPLA provides numerous health services for patients, including testing for sexually transmitted diseases, HIV testing, emergency contraception, family planning procedures, and cancer screenings.

3. On October 17, 2021, PPLA identified suspicious activity on its computer network. Shortly thereafter, PPLA determined that an unauthorized third-party gained access to its network between October 9, 2021, through October 17, 2021. On November 4, PPLA identified the exfiltrated files from its network.

4. The events in paragraphs 1 through 3 are collectively referred to as the "Data Breach."

5. The inadequate protections for patient data are particularly egregious in light of the fact that Planned Parenthood has already experienced data breaches in 2015 and 2020.

6. On November 30, 2021, PPLA reported the Data Breach to the California Attorney General. The notice provides that: "an unauthorized person gained access to our network between October 9, 2021 and October 17, 2021, and exfiltrated some files from our systems during that time." The notice also sets out that: "we identified files that contained your name and one or more

of the following: address, insurance information, date of birth, and clinical information, such as diagnosis, procedure, and/or prescription information" (collectively, the "PII/PHI").[1]

7. The Data Breach affected more than 400,000 PPLA patients.

8. Plaintiff received notice of the data breach in a letter dated November 30, 2021.

9. Defendant owed a duty to Plaintiff and Class members to maintain reasonable and adequate security measures to secure, protect, and safeguard the PII/PHI they collected and stored about them. Defendant breached said duty by failing to implement and maintain reasonable security procedures and practices to protect the PII/PHI from unauthorized access and unnecessarily using, storing, and retaining Plaintiff's and Class members' personal information on its inadequately protected network.

10. Defendant knew that additional security was required to protect Plaintiff's and Class members' personal information. Further, Defendant was aware that it maintained inadequate security procedures, as it had already experienced multiple data breaches since 2015. Thus, Defendant knew that the information uploaded on its network was susceptible to security risks. Nonetheless, Defendant continued to use its inadequate network to store, maintain and transmit extremely sensitive PII/PHI.

11. Due to the Defendant's inadequate cybersecurity, Plaintiff's and Class members' PII/PHI was accessed and disclosed in the Data Breach.

12. Plaintiff brings this action on behalf of herself and all affected consumers in California whose PII/PHI was exposed as a result of the Data Breach. Plaintiff seeks, for herself and the Class, injunctive relief, actual and other economic damages, consequential damages, nominal damages or statutory damages, punitive damages, and attorney's fees, litigation expenses, and costs.

PARTIES

13. Plaintiff Michelle Garza is a resident of Los Angeles, California and has an intent to remain there, and is therefore a domiciliary of California. Plaintiff frequently visits PPLA for

[1]https://oag.ca.gov/system/files/EXPERIAN_H1202_Planned%20Parenthood%20of%20Los%20Angeles_L01_SAS_1.pdf.

medical treatment. As a patient, Plaintiff provided PPLA with her confidential and highly sensitive PII/PHI when she received medical treatment. In or about December 2021, PPLA notified Plaintiff that her PII/PHI was accessed by unauthorized users as a result of the Data Breach.

14. Defendant Planned Parenthood Los Angeles is a California non-profit company headquartered in Los Angeles, California. PPLA provides numerous health services, including testing for sexually transmitted diseases, HIV testing, emergency contraception, family planning procedures, and cancer screenings.

JURISDICTION AND VENUE

15. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiff and Class members pursuant to Cal. Code Civ. Proc. § 382.

16. This Court has personal jurisdiction over Defendant PPLA because it is headquartered in and has its principal place of business in California.

17. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. §§ 395 and 395.5 because Plaintiff and Defendant reside in Los Angeles and all of the actions that gave rise to this Complaint occurred in Los Angeles.

FACTUAL ALLEGATIONS

I. BACKGROUND ON DATA BREACHES

18. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.[2]

19. Data breaches are becoming increasingly more common and harmful. In 2014, 783 data breaches were reported, with at least 85.61 million total records exposed.[3] In 2019, 3,800 data breaches were reported, with at least 4.1 billion total records exposed.[4] The average cost of a data breach in the United States in 2019 was $8.19 million.[5]

---

[2] Julian De Groot, *The History of Data Breaches*, DIGITAL GUARDIAN (Oct. 24, 2019), https://digitalguardian.com/blog/history-data-breaches.

[3] Julian De Groot, *The History of Data Breaches*.

[4] Dan Rafter, *2019 Data Breaches: 4 Billion Records Breached So Far*, NORTON BY SYMANTEC, https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html.

[5] Chris Brook, *What's the Cost of a Data Breach in 2019*, DIGITAL GUARDIAN (July 30, 2019), *https*://digitalguardian.com/blog/whats-cost-data-breach-2019.

20. Consumers are harmed in a variety of ways by data breaches. First, consumers are harmed financially. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[6] However, other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft—a common result of data breaches—was $298 dollars.[7] And in 2019, Javelin Strategy & Research compiled consumer complaints from the U.S. Federal Trade Commission ("FTC") and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[8]

21. Data breaches involving Personal Health Information ("PHI") are even worse. Such data breaches "typically leave[] a trial of falsified information in medical records that can plague victims' medical and financial lives for years."[9] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[10] "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care."[11] And, "[i]f the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[12]

22. As the World Privacy Forum wrote in a report:

> Victims of medical identity theft may receive the wrong medical treatment, find their health insurance exhausted, and could become uninsurable for both life and health insurance coverage. They may fail physical exams for employment due to the presence of diseases in their health record that do not belong to them. It is nightmarish that

[6] *Id*.

[7] NORTON BY SYMANTEC, 2013 NORTON REPORT 8 (2013), https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

[8] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

[9] Pam Dixon, et al., *The Geography of Medical Identity Theft* (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf.

[10] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions*, PUBLIC INTELLIGENCE (May 6, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions/.

[11] *See* FEDERAL TRADE COMMISSION, MEDICAL IDENTITY THEFT, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

[12] *Id.*

> patients' medical records may include information about individuals who have stolen their identities for the purposes of using the victims' insurance or for dodging medical bills.[13]

23. Identity theft is one of the most problematic harms resulting from a data breach. With access to an individual's PII, criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name, but with the thief's picture. In addition, identity thieves may obtain a job, rent a house, or receive medical services in the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[14]

24. Consumers are also harmed by the time they spend rectifying the effects of a data breach. A Presidential identity theft report from 2007 states that:

> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts, open new ones, and dispute charges with individual creditors.[15]

25. Further, the effects of a data breach on consumers are not temporary. In a report issued by the U.S. Government Accountability Office ("GAO"), the GAO found that "stolen data may be held for up to a year or more before being used to commit identity theft," and "fraudulent use of [stolen information] may continue for years" after the stolen information is posted on the Internet.[16] In fact, consumers suffer 33% of the harm from a data breach after the first year.[17] Thus, consumers can lose years' worth of time dealing with a data breach.

---

[13] PAM DIXON, WORLD PRIVACY FORUM, MEDICAL IDENTITY THEFT: THE INFORMATION CRIME THAT CAN KILL YOU, at 6 (2006) http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wpf_medicalidtheft2006.pdf.

[14] *See Warning Signs of Identity Theft*, Federal Trade Commission, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.

[15] U.S. FEDERAL TRADE COMMISSION, THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN 11 (2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf.

[16] *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 694 (7th Cir. 2015) (citing U.S. GOV'T ACCOUNTABILITY OFFICE, GAO–07–737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION (2007)).

26. The existence of these problems is not always immediately ascertainable. As the GAO Report describes:

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

27. Consumers are also harmed by the lost value of their data. Personally Identifying Information ("PII") and Personal Health Information ("PHI") represent important, highly valuable property rights.[18] PII and PHI can be easily commodified, allowing the information to be bought and sold.[19] This information "has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[20]

28. PHI is highly prized because health insurance files contain multiple pieces of highly sensitive information, including health insurance information, names, addresses, telephone numbers, email addresses, and Social Security numbers, and bank account information, including routing numbers. Such information is valued at between $1,200 to $1,300 on the black market.[21] This, according to the Federal Bureau of Investigation's ("FBI") Cyber Division, is the reason healthcare records can be sold by criminals for roughly 50 times higher than the price of a stolen social security or credit card number.[22]

---

[17] Larry Ponemon, *What's New in the 2019 Cost of a Data Breach Report*, SECURITY INTELLIGENCE, https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/.

[18] *See* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[19] *See* Robert Lowes, *Stolen EHR [Electronic Health Records] Charts Sell for $50 Each on Black Market*, MEDSCAPE (April 28, 2014), https://www.medscape.com/viewarticle/824192.

[20] Soma, *supra*, *Corporate Privacy Trend*.

[21] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/home/security-news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/.

[22] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8,2014), https://www.illuminweb.com/wp-conent/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

29. As a result, companies have begun providing an opportunity to consumers to sell this information to advertisers and other third parties. More and more, consumers have control over who ultimately receives their PII/PHI, and when consulted, consumers place a high value on their PII/PHI as well as on the privacy of that information. Researchers have even confirmed that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[23]

30. Thus, when consumers PII/PHI is disclosed without their consent, consumers are deprived of both the ability to choose what is done with their information as well as the full monetary value of their information.

II. DEFENDANT COLLECTED AND FAILED TO SECURE CLASS MEMBERS' INFORMATION

31. PPLA collects a considerable amount of PII and PHI from its patients in order for them to receive treatment.

32. PPLA notifies current and prospective patients of its privacy policy in accordance with HIPPA.[24] The privacy policy can be found on Defendant's website and provides, in part, that "[w]e understand that health information about you and your health care is personal. We are committed to protecting health information about you. [] The privacy and security provisions of the federal Health Insurance Portability and Accountability Act ("HIPPA") require us to: Make sure that health information that identifies you is kept private."

33. As a medical provided, Defendant should have taken reasonable steps to ensure the safety of Plaintiff and putative class members' PPI/PHI.

34. Despite these representations, PPLA failed to operate a secure network, leaving high risk targets like Plaintiff's and the Class's PII and PHI exposed.

35. Planned Parenthood is no stranger to data breaches. The non-profit's network has already been exposed by data breaches in 2015[25] and 2020.[26]

---

[23] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFORMATION SYSTEMS RESEARCH 254, 254 (2011), https://www.jstor.org/stable/23015560?seq=1#page_scan_tab_contents.

[24] https://www.plannedparenthood.org/planned-parenthood-los-angeles/hipaa.

[25] https://www.cnn.com/2015/07/27/politics/planned-parenthood-hacked/index.html.

36. Despite these recent attacks, Defendant failed to take sufficient steps to protect its patients PPI/PHI.

37. On October 9, 2021, an unauthorized party(ies) gained access to PPLA's network. PPLA did not become aware of the Data Breach until October 17, 2021. For eight days, PPLA allowed this unauthorized party to access its network and extract sensitive patient information, including "dates of birth, addresses, insurance identification numbers, and clinical data, such as diagnosis, treatment, or prescription information."[27]

38. The unauthorized third party accessed the stolen information and is certain to use it for improper and nefarious purposes.

39. As such, Defendant was aware that PII and PHI were at high risk of theft. Accordingly, Defendant should have anticipated and taken appropriate and standard measures to protect Plaintiff's and Class member's PII and PHI against cyber-security attacks.

40. It was not until November 30, 2021 that the Defendant filed a notice with the State of California Department of Justice indicating a data breach of unsecured and protected health information of hundreds of thousands of individuals.[28]

41. All told, over 400,000 patients' records were exposed in the Data Breach.

42. Defendant delayed reporting the Data Breach to the California Attorney General until 26 days after it had learned of the patient information exposed by the Data Breach.

43. Defendant's notice of Data Breach failed to provide adequate remediation. PPLA has not offered Plaintiff, or any member of the putative class, any compensation or remediation for the PPI/PHI exposed in connection with the Data Breach. Identity thieves place a high value on PHI (especially when combined with PII). Medical identity theft may take twice as long to discover and the impact can have severe consequences. For instance, thieves may use stolen PHI to see a doctor, get prescription drugs, and file claims. Even more so, if the thief's health information is mixed with the victim's, this can have devastating consequences to a victim's health.

---

[26] https://www.plannedparenthood.org/planned-parenthood-metropolitan-washington-dc/who-we-are/reports-financials/notice-our-patients-regarding-cyber-incident.
[27] https://www.plannedparenthood.org/planned-parenthood-los-angeles/notice.
[28] https://oag.ca.gov/ecrime/databreach/reports/sb24-548069.

44. Defendant's notice of Data Breach further failed to provide sufficient details about what PII/PHI was accessed and by whom. PPLA stated only that the aforementioned information was breached, but failed to provide any specifics, including the time period of the information breached. As noted, it is not clear on the face of Defendant's notice whether this data includes information uploaded in the past year or several past years.

45. In turn, Plaintiff and Class members have been unable to adequately protect themselves against medical and identity theft.

CLASS ALLEGATIONS

46. Pursuant to Cal. Code Civ. Proc. § 382, Plaintiff seeks to represent a class defined as: All patients of PPLA whose PII and PHI was exposed in the Data Breach.

47. Excluded from the Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

48. The class size is estimated to be approximately 400,000 people. Therefore, Plaintiff believes that the Class is so numerous that joinder of all members is impractical.

49. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured in the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arose from the same practices or course of conduct that give rise to the claims of all Class members.

50. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

(a) Whether Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII/PHI they collected from Plaintiff and Class members;

(b) Whether Defendant breached its duty to protect the PII/PHI of Plaintiff and each Class member; and

(c) Whether Plaintiff and each Class member are entitled to statutory damages, actual damages and other equitable relief.

51. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests that are adverse to or that conflict with the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

52. Further, a class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder all Class members is impractical. Additionally, the expense and burden of individual litigation would make it difficult or impossible for the individual Class members to redress the wrongs done to them, especially given the costs and risks of litigation as compared to the benefits that may be attained. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefit of single adjudication and comprehensive supervision by a single forum.

53. Finally, Defendant has acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive relief and declaratory relief with respect to the Class as a whole.

COUNT I
Violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56, *et seq.*

54. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

55. Plaintiff brings this claim on behalf of herself and the Class against Defendant.

56. Section 56.10(a) of the California Civil Code states that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of

the provider of health care or an enrollee of a health care service plan without first obtaining an authorization."

57. This section is complemented by California Civil Code, Section 56.10(d) which provides that:

> Except to the extent expressly authorized by a patient, enrollee, or subscriber, or as provided by subdivision (b) and (c), a provider of health care, health service plan, contractor, or corporation and its subsidiaries and affiliates shall not intentionally share, sell, use for marketing, or otherwise use medical information for a purpose not necessary to provide health care services to the patient.

58. California Civil Code, Section 56.10(e) contains a similar prohibition:

> A contractor or corporation and its subsidiaries and affiliates shall not further disclose medical information regarding a patient of the provider of health care or an enrollee or subscribers of a health care service plan or insurer or self-insured employer received under this section to a person or entity that is not engaged in providing health care services to the patient.

59. PPLA is a "provider of health care" and/or "service plan[s]" within the meaning of Civil Code § 50.06 and is an entity regulated pursuant to the Knox-Keene Health Care Service Plan of 1975, and are therefore subject to the requirements of the CMIA.

60. Plaintiff and all members of the Class are "patients" within the meaning of Civil Code § 56.06(k) and are "endanger[ed]" within the meaning of Civil Code § 56.06(e) because Plaintiff and the Class fear that disclosure of their medical information will subject them to harassment or abuse.

61. Plaintiff and the respective Class members, as patients, had their individually identifiable "medical information"—within the meaning of Civil Code § 56.05(j)—created, maintained, preserved, stored, abandoned, destroyed, or disposed of on and/or via Defendant's computer networks at the time of the Data Breach.

62. Defendant, through inadequate security, allowed an unauthorized third party to gain access to, view and/or download Plaintiff's and each Class member's medical information, without the prior written authorization of Plaintiff and the Class members, as required by Civil Code § 56.10 of the CMIA.

63. In violation of Civil Code § 56.10(a), PPLA affirmatively disclosed Plaintiff's and

Class members' medical information without first obtaining an authorization. Specifically, PPLA continued to store data on its outdated and insecure network, despite experiencing multiple data breaches in recent years, which in turn was accessed by hackers.

64. Plaintiff's and Class member's medical information was viewed by unauthorized individuals as a direct and proximate result of PPLA's violation of Civil Code § 56.10(a). PPLA's notice of data breach to Plaintiff confirmed that her PII/PHI was compromised, as described herein.

65. The conclusion that Plaintiff's and Class member's PII/PHI was actually viewed also flows logically from the particulars of a data breach. "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015); *see also Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) ("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints.").

66. In violation of Civil Code § 56.10(a), PPLA disclosed medical information pertaining to members of the proposed Class to unauthorized persons without first obtaining consent. PPLA continued to actively use, upload and transfer sensitive files onto its network, despite its knowledge that the network lacked adequate security to protect its members' PII and PHI.

67. Such actions resulted in the disclosure or information to and its viewing by unauthorized individuals in the Data Breach in violation of Civil Code § 56.10(a).

68. In violation of Civil Code § 56.10(e), Defendant disclosed Plaintiff's and Class members' medical 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.

69. Defendant further violated § 56.101 of the CMIA through its failure to maintain and preserve the confidentiality of Plaintiff's and the Class member's medical information.

70. In violation of Civil Code § 56.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and Class member's medical information in a manner that failed to preserve the confidentiality of the information contained therein. Plaintiff's and Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

71. In violation of Civil Code § 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and Class members' medical information. Plaintiff's and Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a). PPLA's notice of data breach to Plaintiff confirmed the information was viewed, as described herein.

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

73. In violation of Civil 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. Plaintiff's and Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(b)(1)(A).

74. Defendant violated Civil Code § 56.36 of the CMIA through its failure to maintain and preserve the confidentiality of Plaintiff's and the Class' medical information.

75. As a result of Defendant's above-described conduct, Plaintiff and the Class have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36.

76. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an

imminent, immediate and continuing increased risk of identity theft, identity fraud, and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) invasion of privacy; (iii) breach of the confidentiality of their PII/PHI; (iv) statutory damages under the California CMIA; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

77. Plaintiff, individually, and each member of the Class, seek statutory damages of one thousand dollars ($1,000) for each violation of Civil Code § 56.36(b)(1), actual damages suffered pursuant to Civil Code § 56.36(b)(2), injunctive relief, and punitive damages of up to $3,000 per Plaintiff and each Class member, attorney's fees, litigation expenses, and court costs pursuant to § 56.35.

COUNT II
Violation of the California Customer Records Act (CCRA)
Cal. Civ. Code §§ 1798.80, *et seq.*

78. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

79. Cal. Civ. Code § 1798.80(a) defines a "business" as "a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit."

80. Cal. Civ. Code § 1798.80(c) defines a "customer" as "an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business."

81. Cal. Civ. Code § 1798.80(e) defines "personal information" as:

> …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…address, telephone number…insurance policy number…any other financial information, medical information, or health insurance information.

82. Cal. Civ. Code § 1798.82 provides:

> (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a 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 person or business 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, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

83. Defendant is a "business" within the meaning of Cal. Civ. Code § 1798.80(a).

84. Plaintiff and members of the Class are "customers" within the meaning of Cal. Civ. Code § 1798.80(c).

85. Plaintiff and Class member's PPI/PHI is "personal information" within the meaning of Cal. Civ. Code § 1798.80(e).

86. Defendant first became aware of the Data Breach on October 17, 2021. Defendant did not notify Plaintiff and members of the Class of the Data Breach until November 30, 2021. In violation of Cal. Civ. Code § 1798.82, Defendant failed to provide Plaintiff and members of the Class reasonable notice of the Data Breach.

87. Timely notice was necessary so that Plaintiff and members of the Class could take proactive measures to mitigate the dangers of their information being stolen.

88. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CCRA, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and continuing increased risk of identity theft, identity fraud, and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled

to compensation; (ii) invasion of privacy; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

89. Plaintiff and members of the Class seek actual damages under Cal. Civ. Code § 1798.84(b), injunctive and declaratory relief, and any other relief deemed appropriate by the Court.

COUNT III
Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq.*

90. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

91. Defendant has violated Cal. Bus. & Prof. Code § 17200, et seq. by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitutes acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to Plaintiff and members of the Class.

92. 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 Plaintiff's and members of the Class' PPI/PHI with the knowledge that such information would not be adequately protected; and by storing Plaintiff's and members of the Class' PPI/PHI in an unsecure environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods of safeguarding PPI/PHI.

93. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

94. Plaintiff and members of the Class were injured as a direct and proximate result of Defendant's unlawful practices and acts, including but not limited to: (i) an imminent, immediate and continuing increased risk of identity theft, identity fraud, and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) invasion of privacy; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value

of their PII/PHI, for which there is a well-established national and international market; and/or (v) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

95. Defendant knew or should have known that its network was inadequate to safeguard Plaintiff's and members of the Class' PPI/PHI and that the risk of data breach or theft was highly likely, especially considering the recent data breaches Defendant has experienced.

96. Plaintiff and members of the Class are entitled to damages in an amount to be proven at trial, and to equitable relief, including injunctive relief.

COUNT IV
Negligence

97. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

98. Defendant had and continues to have a duty to Plaintiff and members of the Class to safeguard and protect their PPI/PHI. Defendant created this duty by requiring Plaintiff and members of the Class to provide their PPI/PHI in order to receive medical treatment. Defendant collected and stored Plaintiff and Class members PPI/PHI for the purposes of providing medical treatment.

99. Defendant's duty required it, among other things, to design and employ cybersecurity systems, anti-hacking technologies and intrusion detection and reporting systems sufficient to protect the PPI/PHI from unauthorized access and to promptly alert Defendant to any such access and enable it to determine the extent of any compromised PPI/PHI.

100. Had Defendant adequately designed, employed, and maintained appropriate technological and other systems, the PPI/PHI would not have been compromised or, at a minimum, Defendant would have known of the unauthorized access sooner and would be able to accurately inform Plaintiff and the other members of the Class of the extent to which their PPI/PHI has been compromised.

101. Defendant breached its duty of care by, among other things, failing to maintain appropriate technological and other systems to prevent unauthorized access, failing to minimize the

PPI/PHI that any intrusion could compromise, and failing to detect the Data Breach in a timely manner to avoid or minimize the effects of the Data Breach.

102. Defendant's breach of its duty provided the means for the unauthorized third party to access, obtain, and potentially misuse the PPI/PHI of Plaintiff and the members of the Class without authorization. It was reasonably foreseeable that such breaches would expose the PPI/PHI to criminals and other unauthorized users.

103. Defendant's breach of its duty has directly and proximately injured Plaintiff and members of the Class, including but not limited to: (i) an imminent, immediate and continuing increased risk of identity theft, identity fraud, and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) invasion of privacy; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

104. Plaintiff and members of the Class are entitled to damages in an amount to be proven at trial, and to equitable relief, including injunctive relief.

COUNT V
Breach of Implied Contract

105. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

106. Plaintiff and members of the Class were required to provide Defendant their PPI/PHI in order to receive medical treatment.

107. In doing so, Plaintiff and members of the Class entered into an implied contract with Defendant, whereby Defendant agreed to safeguard and protect the PPI/PHI of Plaintiff and members of the Class and to only use such information for medical treatment.

108. When entering into this implied contract, Plaintiff and members of the Class reasonably believed that Defendant would safeguard and protect their PPI/PHI and only use such information for medical treatment.

109. Plaintiff and members of the Class would not have provided such highly sensitive information in the absence of Defendant's implied promise to safeguard and protect their PPI/PHI.

110. Plaintiff and members of the Class fully performed their obligations to Defendant by providing their PPI/PHI and fully paying for the medical treatment they received.

111. Defendant breached its implied contract with Plaintiff and members of the Class by failing to safeguard and protect their PPI/PHI from unauthorized third parties.

112. As a direct and proximate result of Defendant's breach, Plaintiff and members of the class have suffered damages, including but not limited to: (i) an imminent, immediate and continuing increased risk of identity theft, identity fraud, and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) invasion of privacy; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

113. Plaintiff and members of the Class are entitled to damages in an amount to be proven at trial, and to equitable relief, including injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all members of the Class, seeks judgment against Defendant, as follows:

(a) An Order certifying the proposed Class and appointing Plaintiff and her Counsel to represent the Class;

(b) An Order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and the Class's PII/PHI;

(c) An Order compelling Defendant to employ and maintain appropriate systems and policies to protect consumer PII/PHI and to promptly detect, and timely and accurately report, any unauthorized access to that data;

(d) An award of compensatory, statutory, and punitive damages, in an amount to be determined;

(e) An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law;

(f) Interest on all amounts awarded, as allowed by law; and

(g) Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: December 28, 2021

Respectfully submitted,

BURSOR & FISHER, P.A.

By: L. Timothy Fisher
L. Timothy Fisher

L. Timothy Fisher (State Bar No. 191626)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ltfisher@bursor.com

Attorneys for Plaintiff