Adam E. Polk (State Bar No. 273000)
Simon Grille (State Bar No. 294914)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
apolk@girardsharp.com
sgrille@girardsharp.com

Counsel for Plaintiff

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

K.O., individually and on behalf of all others similarly situated,

Plaintiff,

vs.

PLANNED PARENTHOOD LOS ANGELES,

Defendant.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff K.O. ("Plaintiff"), individually and on behalf of the proposed class defined below, brings this action against Defendant Planned Parenthood Los Angeles ("Planned Parenthood" or "PPLA"), and allege as follows:

I. SUMMARY OF THE ACTION

1. This action arises out of Planned Parenthood's failure to secure the highly sensitive personal information of its patients, including those who visited Planned Parenthood for reproductive or sexual health services. Between approximately October 9, 2021, and October 17, 2021, an unauthorized party or parties accessed Planned Parenthood's computer network, installed ransomware, and exfiltrated patient files (the "Data Breach"). On or about October 17, Planned Parenthood learned of the breach and that the files extracted contained patient names, dates of birth, addresses, insurance identification numbers, and clinical data, such as diagnosis, treatment, or prescription information. Over 400,000 patients' personally identifiable information ("PII") and personal health information ("PHI") was compromised in the attack. Planned Parenthood did not protect this sensitive patient data despite being previously hacked, in both 2015 and 2020. Further, although Planned Parenthood learned of this hack on October 17, 2021, it did not notify patients of the attack until November 30, 2021. The personal information remains in the possession of the unauthorized party or parties.

2. By its nature, the information exfiltrated in the Data Breach is extremely sensitive: Planned Parenthood provides not only abortion and other family planning procedures, but also such health services as testing for sexually transmitted diseases, HIV testing, emergency contraception, and cancer screenings. Because Planned Parenthood provides these highly private services—and because it has become a lightning rod for the public debate around abortion restrictions—the exfiltrated information, including Plaintiff's identity, is of the utmost sensitivity. Particularly given its highly confidential nature, the information compromised in the Data Breach is valuable to hackers, who may try to sell it on the black market. The breach also occurred at a moment when the constitutionality of certain abortion laws is under attack

and Planned Parenthood has been the target of many protests and threats. The timing of this hack makes it more likely that hackers will exploit the stolen information or seek ransom payments for its return. The Data Breach is particularly egregious in light of the numerous high-profile security attacks and data breaches that have occurred recently, including in the healthcare industry.

3. As a result of Planned Parenthood's data security failures, Plaintiff and the members of the Class proposed in this case confront a significant threat of identity theft and other harm—imminently and for years to come. Plaintiff by this action seeks compensatory and statutory damages, together with injunctive relief to remediate Planned Parenthood's deficient cybersecurity protocols and provide identity theft insurance (or the money needed to secure those services) to protect her and the other breach victims from identity theft and fraud.

II. PARTIES

4. Plaintiff is a citizen and resident of Glendale, California. Plaintiff is using her initials in this litigation to protect her privacy, and if required by the Court, will seek permission to proceed under this pseudonym.

5. Defendant Planned Parenthood Los Angeles is a California corporation with its principal place of business in Los Angeles, California.

III. JURISDICTION AND VENUE

6. This Court has jurisdiction over the lawsuit under the Class Action Fairness Act, 28 U.S.C. § 1332, because this is a proposed class action in which: (1) there are at least 100 class members; (2) the combined claims of class members exceed $5,000,000, exclusive of interest, attorneys' fees, and costs; and (3) Defendant and class members are domiciled in different states.

7. This Court has personal jurisdiction over Defendant because it is incorporated in and has its principal place of business in California.

8. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant's principal place of business is within this District and a substantial part of the events or omissions giving rise to the claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Plaintiff's Private Health Information Was Hacked, Causing Damage

9. Plaintiff began receiving healthcare services from Planned Parenthood in 2014 and continues to receive such services from Planned Parenthood.

10. In order to receive these healthcare services, Plaintiff provided Planned Parenthood with personally identifying and health information including her name, address, health insurance information and date of birth. Plaintiff also provided Planned Parenthood with sensitive information concerning her personal medical history.

11. Around November 30, 2021, Plaintiff received a letter from Planned Parenthood informing her of the data breach and advising her to take protective measures. The letter stated that Planned Parenthood experienced suspicious activity on its computer network and an unauthorized party or parties removed files from its system. The letter informed Plaintiff that the files contained her name, and one or more of the following: her address, insurance information, date of birth, and clinical information such as diagnosis, procedure, and/or prescription information.

12. Plaintiff suffers from stress and anxiety as a result of the Data Breach and from the loss of her privacy.

13. On December 9, 2021, Plaintiff received an alert from Experian notifying her that her that Experian found an unfamiliar address associated with her Social Security number. The alert characterized the "risk level" as "high."

14. Plaintiff also suffered injury in the form of damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff entrusted to Planned Parenthood and which was compromised as a result of the Data Breach it failed to prevent.

15. Plaintiff suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from her personal information—especially her diagnosis, treatment, or prescription information—being placed in the hands of unauthorized third parties.

16. Plaintiff has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Planned Parenthood Suffered a Foreseeable Data Breach

17. Planned Parenthood is an affiliate of Planned Parenthood Federation of America (or "PPFA"). PPFA is a nonprofit organization that delivers reproductive health care, sex education, and information to millions of people worldwide. PPFA is the nation's largest provider of sexual education, and the nation's leading provider of sexual and reproductive health. PPFA holds itself out as America's most trusted provider of sexual and reproductive health care.

18. PPFA has 49 independent, local affiliates that operate over 600 health centers around the United States, each of which provides health care services and sexual education programs.

19. Planned Parenthood Los Angeles is one of these affiliates and offers a range of reproductive health care services to women, men, and teens throughout Los Angeles. Planned Parenthood is one of the largest providers of reproductive health care in Los Angeles County and operates 21 health centers throughout Los Angeles.

20. As one of the largest providers of comprehensive, reproductive health in Los Angeles County, Planned Parenthood conducts more than 250,000 visits at its 21 health care centers per year. Planned Parenthood offers the following services to its patients:

a. Annual Exams

b. Birth Control, including IUDs and Implants

c. Breast Cancer Screenings

d. Cervical Cancer Screenings

e. Contraceptive Counseling & Management
f. HPV Vaccine
g. Morning-After Pill (Emergency Contraception)
h. Prenatal Care
i. PrEP and PEP
j. Sexual Education
k. Testicular Cancer Screenings
l. Pap Tests
m. Pregnancy Testing & Options Counseling
n. HIV Testing and Referral
o. Testing & Treatment for:
    i. Sexually Transmitted Infections (STIs)
    ii. Urinary Tract Infections (UTIs)
    iii. Vaginal Infections
p. Abortion Services (Surgical and Medication)
q. Colposcopy and LEEP
r. Vasectomy

21. Under the federal Health Insurance Portability and Accountability Act ("HIPAA"), Planned Parenthood is required to ensure that health information that identifies patients is kept private and notify patients when a breach occurs.

22. Planned Parenthood's HIPAA Privacy Policy states that it is "committed to protecting health information about [patients]" because [it] understand[s] that health information about [patients and their health care] is personal.[1]

23. Planned Parenthood's HIPAA policy additionally states the following: "Our pledge regarding your health information is backed-up by federal and state law. The

[1] https://www.plannedparenthood.org/planned-parenthood-los-angeles/hipaa (last visited Dec. 8, 2021).

privacy and security provisions of the federal Health Insurance Portability and Accountability Act ("HIPAA") require us to:

- Make sure that health information that identifies you is kept private;
- Make available this notice of our legal duties and privacy practices with respect to health information about you; and
- Follow the terms of the notice that is currently in effect."[2]

24. Planned Parenthood acknowledges on its website that it is "required by federal and state law to notify" patients following a breach with respect to unsecured protected health information.[3] Although Planned Parenthood identified the Data Breach on October 17, 2021, it did not inform patients of the breach until November 30, 2021.

25. Between October 9, 2021, and October 17, 2021, an unauthorized party or parties gained access to Planned Parenthood's network, installed ransomware systems, and withdrew patient files, compromising information for over 400,000 patients.

26. On November 4, 2021, Planned Parenthood learned that breached files contained patients' names and one or more of the following: address, insurance information, date of birth, and clinical information, such as diagnosis, procedure, and/or prescription information.

27. On November 30, 2021, Planned Parenthood notified patients of the breach and advised them to take protective measures.

28. This is not the first breach affecting Planned Parenthood affiliates. In 2015, anti-abortion activists gained access to the names and emails of hundreds of employees and posted them online. Again in 2020, Planned Parenthood announced that patient and donor information had been hacked from its Washington, D.C. affiliate.

29. The private health information taken from Planned Parenthood's system is particularly sensitive for several reasons. First, medical information is valuable to

[2] *Id.*

[3] *Id.*

cybercriminals and has routinely been sold and traded on the dark web. Second, patients who were seen at Planned Parenthood now have their most private information exposed, which can include a person's HIV status, test results for sexually transmitted diseases, information surrounding pregnancy and termination, and cancer screenings. Third, given the political and legal controversy surrounding abortion and its constitutionality, this compromised medical information is even more sensitive and capable of being exploited.

Personally Identifiable Information Has Concrete Financial Value

30. PII and PHI are inherently valuable and the frequent target of hackers. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018. Of the 1,473 recorded data breaches, 525 of them, or 35.64% were in the medical or healthcare industry. The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.

31. Identity theft results in a significant negative financial impact on victims as well as severe distress.

32. Planned Parenthood is aware that the PII and PHI it collects is highly sensitive and of substantial value to those who would use it for wrongful purposes.

33. PII and PHI is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud. There is a robust black market in which criminals openly post stolen PII and PHI on multiple underground internet websites, commonly referred to as the dark web.

34. There is accordingly a market for Plaintiff's and Class members' PII and PHI, and her stolen PII and PHI has inherent value. Sensitive healthcare data can sell for as much as $363 per record, according to the Infosec Institute.

35. PHI is particularly valuable because criminals can use it to target victims

with fraud and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

36. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, misdiagnosis or mistreatment can ensue. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[4]

37. The detrimental consequences of Planned Parenthood's failure to keep its patients' PII and PHI secure are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

38. Criminals often trade stolen PII and PHI on the "cyber black market" for years following a breach. Cybercriminals also can post stolen PII and PHI on the internet, thereby making the information publicly available without the knowledge or consent of the victim.

39. Planned Parenthood knew the importance of safeguarding the PII and PHI entrusted to it and the foreseeable adverse effects if its data security systems were breached. Those effects include the significant costs that would be imposed on Planned Parenthood's patients as a result of a breach. Planned Parenthood failed to implement adequate cybersecurity measures, leading to the Data Breach.

[4] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/ (last visited Dec. 8, 2021).

V. CLASS ACTION ALLEGATIONS

40. Plaintiff brings this lawsuit as a class action on her own behalf and on behalf of all other persons similarly situated as members of the proposed Class, pursuant to Federal Rules of Civil Procedure 23(a) and (b)(2) and (3). This action satisfies the numerosity, commonality, typicality, predominance, and superiority requirements.

41. The proposed Class and Subclass are defined as:

> **Class**
> All United States citizens and residents whose personally identifiable information was in Planned Parenthood's electronic information systems and was compromised as a result of the October 2021 breach.
>
> **California Subclass**
> All California citizens and residents whose personally identifiable information was in Planned Parenthood's electronic information systems and was compromised as a result of the October 2021 breach.

42. Excluded from the Class are Defendant and its officers, directors, and managerial employees. Also excluded are individuals employed by counsel for the parties in this action and any Judge to whom this case is assigned, as well as his or her staff and immediate family.

43. Plaintiff reserves the right to modify, change, or expand the Class definition, including by proposing subclasses, based on discovery and further investigation.

44. Numerosity. While the exact number of Class members is not known at this time, the Class is so numerous that joinder of all members is impractical. Over 400,000 patients' medical information was compromised in this attack. The identities of Class members are available through information and records in the possession, custody, or control of Defendant, and notice of this action can be readily provided to the Class.

45. Typicality. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all Class members, had her PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions of Defendant described herein. Plaintiff's claims thus arise from the same course of conduct that gives rise to the claims of all Class members.

46. Adequacy of Representation. Plaintiff is a member of the proposed Class and will fairly and adequately represent and protect the other members' interests. Plaintiff's counsel are competent and experienced in class action and privacy litigation and will pursue this action vigorously. Plaintiff has no interests adverse to the interests of other Class members.

47. Predominant Common Issues of Law and Fact. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual Class members. Among the questions of law and fact common to the Class are:

a. Whether Defendant had a duty to implement reasonable cybersecurity measures to protect Plaintiff's and Class members' sensitive personal information and to promptly alert them if such information was compromised;

b. Whether Defendant breached its duties by failing to take reasonable precautions to protect Plaintiff's and Class members' sensitive personal information;

c. Whether Defendant acted negligently by failing to implement reasonable data security practices and procedures;

d. Whether Defendant violated the California Confidentiality of Medical Information Act, Civ. Code § 56, *et seq*. and/or the California Consumer Records Act, Civ. Code § 1798.80, *et seq*.

e. Whether Defendant's failures to implement reasonable data security protocols and to timely notify Plaintiff and Class members of the Data Breach violate the Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq*.; and

f. Whether Plaintiff and Class members are entitled to statutory damages, actual damages, and/or injunctive and other relief in equity.

48. Superiority. This class action is superior to other alternatives for the fair and efficient adjudication of this controversy. Absent a class action, most members of the Class would find the cost of litigating their claims individually to be prohibitively high and would have no effective remedy. Class treatment will conserve judicial resources, avoid waste and the risk of inconsistent rulings, and promote efficient adjudication before a single Judge.

49. Classwide declaratory, equitable, and injunctive relief is appropriate under Rule 23(b)(2) because Defendant has acted on grounds that apply generally to the Class, and inconsistent adjudications would establish incompatible standards and substantially impair the ability of Class members and Defendant to protect their respective interests. Classwide relief assures fair, consistent, and equitable treatment of Class members and Defendant.

FIRST CAUSE OF ACTION

Violation of the California Confidentiality of Medical Information Act Civ. Code § 56, *et seq*. (CMIA)

50. Plaintiff incorporates and realleges the foregoing allegations of fact.

51. Under section 56.10(a) of the Civil Code, "[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 or subscriber of a health care service plan without first obtaining an authorization[.]"

52. Planned Parenthood is a "provider of health care" as defined in Civil Code sections 56.06. Planned Parenthood is organized in part for the purpose of maintaining medical information to make it available to an individual or provider of health care for purposes of information management, diagnosis, or treatment. Planned Parenthood operates medical centers, maintains electronic health care records, and provides health care services and plans. In addition, under subdivision (b) of section 56.06, Planned

Parenthood provides software that is designed to maintain medical information in order to make such information available to individuals or a provider of health care at the request of the individual or a provider of health care, for the purpose of diagnosis, treatment, or management of a medical condition of the individual. Planned Parenthood patients have access to the Planned Parenthood Direct app, in which they are able to request birth control prescriptions. Patients may also use a "patient portal" to communicate with a patient's care team, view and manage appointments, request prescriptions or view medications, view medical records and lab results, and complete health forms online.

53. Plaintiff and Class members are "patients" within the meaning of Civil Code section 56.05(k), and are "endanger[ed]" within the meaning of Civil Code section 56.05(e) because Plaintiff and Class members reasonably fear that disclosure of their medical information could subject them to abuse, extortion, or other harassment or harm.

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

55. Defendant, through its failure to implement and maintain reasonable security procedures and practices, allowed unauthorized persons to gain access to, view, and/or download Plaintiff's and Class members' medical information without their consent in violation of Civil Code section 56.10(a).

56. In violation of Civil Code section 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, their providers of health care, their health care service plans, or their insurers or self-insured employers.

57. By continuing to use its vulnerable networks despite similar breaches occurring to Planned Parenthood affiliates within recent years, Planned Parenthood took

affirmative actions that resulted in the disclosure of Plaintiff's and Class members' medical information under its care.

58. Defendant also violated Civil Code section 56.101 by failing to maintain and preserve the confidentiality of Plaintiff's and Class members' medical information.

59. In violation of Civil Code section 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and Class members' medical information in a manner that failed to preserve the security of that information and breached its confidentiality.

60. Medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as defined by Civil Code section 56.101(c).

61. In violation of Civil Code section 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.

62. Defendant also violated Civil Code section 56.36(b) by negligently releasing Plaintiff's and Class members' confidential information.

63. Defendant's wrongful conduct, actions, inaction, omissions, and want of ordinary care violate the CMIA and directly and proximately caused the Data Breach. Plaintiff's and Class members consequently have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their medical information; (2) loss of the opportunity to control how their medical information is used; (3) diminution in the value and use of their medical information entrusted to Defendant with the understanding that Defendant would safeguard it against theft and not allow it to be accessed and misused by third parties; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identity theft and misuse of their medical information; (5) continued undue risk to their medical information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of

their medical information being stolen in the Data Breach.

64. Plaintiff and Class members were injured and have suffered damages, as described above, from Defendant's illegal disclosure and negligent release of their medical information in violation of Civil Code sections 56.10, 56.36, and 56.101, and accordingly are entitled to relief under Civil Code sections 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000 per violation, injunctive relief, and attorney fees, expenses and costs.

SECOND CAUSE OF ACTION

Violation of the California Consumer Records Act, Civ. Code § 1798.80, *et seq.* (CCRA)

65. Plaintiff incorporates and realleges the foregoing allegations of fact.

66. Plaintiff and California Subclass members are "customers" within the meaning of Civil Code section 1798.80(c), as they provided personal information to Defendant for the purpose of obtaining services from Defendant.

67. Civil Code section 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." Accordingly, Defendant is a "business" within the meaning of Civil Code section 1798.80(a).

68. The CCRA provides that "[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 . . . whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person . . . in the most expedient time possible and without unreasonable delay[.]" Civ. Code § 1798.82.

69. The Data Breach was a breach of security within the meaning of section 1798.82. PII stolen in the Data Breach, such as full names, addresses, insurance information, dates of birth, and clinical information, such as diagnosis, procedure,

and/or prescription information, constitutes "personal information" within the meaning of section 1798.80.

70. In violation of the CCRA, Defendant unreasonably delayed in notifying Plaintiff and Class members of the Data Breach. Defendant was aware of Data Breach by October 17, 2021, but did not notify patients of the Data Breach until on or around November 30, 2021.

71. Timely disclosure was necessary so that Plaintiff and Class members could, among other things: (1) purchase identity protection, monitoring, and recovery services; (2) intensively monitor their credit reports, financial accounts, and other records; and (3) take other steps to protect themselves and attempt to avoid or recover from identity theft.

72. As a result of Defendant's unreasonable delay in notifying Plaintiff and Class members of the Data Breach, they were deprived of an opportunity to take timely and appropriate self-protective measures. In addition, as a result of the delay, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their personal information; (2) loss of the opportunity to control how their personal information is used; (3) diminution in the value and use of their personal information entrusted to Defendant with the understanding that Defendant would safeguard it against theft and not allow it to be accessed and misused by third parties; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identity theft and misuse of their personal information; (5) continued undue risk to their personal information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach, and (7) public discomfort from the exfiltration of their sensitive medical records and information.

73. Therefore, on behalf of the California Subclass, Plaintiff seeks actual damages under Civil Code section 1798.84(b), injunctive and declaratory relief, and any other relief deemed appropriate by the Court.

THIRD CAUSE OF ACTION

Violation of the Unfair Competition Law,

Bus. & Prof. Code § 17200 *et seq.* (UCL)

74. Plaintiff incorporates and realleges the foregoing allegations of fact.

75. The UCL proscribes "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

Unlawful Prong

76. Planned Parenthood's conduct is unlawful, in violation of the UCL, because it violates HIPAA, the CMIA and the CCRA.

77. Planned Parenthood's conduct violates the CMIA for the reasons identified in the first cause of action, *supra*.

78. Planned Parenthood's conduct violates the CCRA for the reasons identified in the second cause of action, *supra*.

79. As a healthcare provider, Planned Parenthood is subject to the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (together, the "Privacy and Security Rules").

80. The Privacy and Security Rules establish a national set of standards for the protection of "individually identifiable health information" that is held or transmitted by a health care provider, which HIPAA refers to as "protected health information."

81. Pursuant to HIPAA, Planned Parenthood must maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI.

82. HIPAA imposes general security standards, which Planned Parenthood failed to meet, including:

a. Ensuring the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits, 45 C.F.R. § 164.306(a);

b. Protecting against any reasonably anticipated threats or hazards to the security or integrity of such information, 45 C.F.R. § 164.306(a);

c. Protecting against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA, 45 C.F.R. § 164.306(a); and

d. Reviewing and modifying the security measures implemented under HIPAA as needed to continue provision of reasonable and appropriate protection of electronic protected health information, 45 C.F.R. § 164.306(e).

83. Planned Parenthood also failed to:

a. Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, 45 C.F.R. § 164.312(a);

b. Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed, 45 C.F.R. § 164.312(d); and

c. Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network, 45 C.F.R. § 164.312(e).

84. Under the HIPAA Privacy Rule, Planned Parenthood may not use or disclose PHI or confidential medical information except as expressly permitted. 45 CFR 164.502(a).

Unfair Prong

85. Planned Parenthood's conduct also is unscrupulous, oppressive and outrageous in violation of the UCL's unfair prong. Planned Parenthood's unfair business acts and practices include:

a. failing to adequately secure the personal information of Plaintiff and Class members from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about Plaintiff and Class members in a manner highly offensive to a reasonable person;

c. enabling the disclosure of personal and sensitive facts about Plaintiff and Class members without their informed, voluntary, affirmative, and clear consent; and

d. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiff and Class members from taking timely self-protection measures.

86. The gravity of harm resulting from Planned Parenthood's unfair conduct outweighs any potential utility. The failure to adequately safeguard personal, extremely sensitive information harms the public at large and is part of a common and uniform course of wrongful conduct.

87. The harm from Planned Parenthood's conduct was not reasonably avoidable by patients. The individuals affected by the Data Breach—by and large, individuals in need of reproductive health care and sexual health services—were required to provide their PII in order to receive such services. Plaintiff and Class members did not know of, and had no reasonable means of discovering, that their information would be exposed to hackers through inadequate data security measures.

88. There were reasonably available alternatives that would have furthered Planned Parenthood's interests in providing health services while protecting PII, such as ensuring best practices in cybersecurity defense, enhancing security measures, and increasing network monitoring.

89. As a direct and proximate result of Planned Parenthood's unfair and unlawful acts or practices, Plaintiff and Class members lost money or property because their highly sensitive personal information experienced a diminution of value, and because they devoted additional time—which they otherwise would or could have devoted to pecuniary gain—to monitoring public records for exposure of their health information.

90. Plaintiff and Class members therefore seek all appropriate relief, including restitution, injunctive relief, civil penalties, and attorneys' fees and costs under Code of Civil Procedure section 1021.5.

FOURTH CAUSE OF ACTION

Negligence

91. Plaintiff incorporates and realleges the foregoing allegations of fact.

92. Defendant collected and stored Plaintiff's and Class members' personal information, including their full names, addresses, insurance information, dates of birth, and clinical information, such as diagnosis, procedure, and/or prescription information.

93. Defendant owed Plaintiff and Class members a duty of reasonable care to preserve and protect the confidentiality of their personal information that they collected. This duty included, among other obligations, maintaining and testing their security systems and computer networks, and taking other reasonable security measures to safeguard and adequately secure the personal information of Plaintiff and the Class from unauthorized access and use.

94. Defendant's duties also arise by operation of statute. The Customer Records Act, Civ. Code § 1798.80 *et seq*., imposes a mandatory duty on Planned Parenthood to implement and maintain reasonable security procedures and practices to safeguard and protect against the unauthorized disclosure of personal information.

95. Plaintiff and Class members were the foreseeable victims of Defendant's inadequate and ineffectual cybersecurity. The natural and probable consequence of

Defendant's failing to adequately secure their information networks was Plaintiff's and Class members' personal information being hacked.

96. Defendant knew or should have known that Plaintiff's and Class members' personal information was an attractive target for cyber thieves, particularly in light of data breaches experienced by other Planned Parenthood entities, as well as data breaches affecting other medical and non-medical entities. The harm to Plaintiff and Class members from exposure of their extremely confidential personal information was reasonably foreseeable to Defendant.

97. Defendant had the ability to sufficiently guard against data breaches by implementing adequate measures to protect its networks, such as by ensuring best practices in cybersecurity defense, enhancing its security measures, and increasing network monitoring.

98. Defendant breached its duty to exercise reasonable care in protecting Plaintiff's and Class members' personal information by failing to implement and maintain adequate security measures to safeguard Plaintiff's and Class members' personal information, failing to monitor its systems to identify suspicious activity, and allowing unauthorized access to, and exfiltration of, Plaintiff's and Class members' highly confidential personal information. Planned Parenthood had knowledge that similar breaches have occurred to Planned Parenthood recently.

99. Defendant also owed a duty to timely disclose to Plaintiff and Class members that their personal information had been or was reasonably believed to have been compromised. Timely disclosure was necessary so that Plaintiff and Class members could, among other things: (1) purchase identity protection, monitoring, and recovery services; (2) monitor their credit reports, financial accounts, and other records; and (3) take other steps to protect themselves and attempt to avoid or recover from identity theft.

100. Defendant breached its duty to timely disclose the Data Breach to Plaintiff and Class members. After learning of the Data Breach, Defendant unreasonably delayed

in notifying Plaintiff and Class members of the Data Breach. This unreasonable delay caused foreseeable harm to Plaintiff and Class members by preventing them from taking timely self-protection measures in response to the Data Breach.

101. There is a close connection between Defendant's failure to employ reasonable security protections for its employees' personal information and the injuries suffered by Plaintiff and Class members. When individuals' extremely sensitive personal information is stolen, they face a heightened risk of identity theft and may need to: (1) purchase identity protection, monitoring, and recovery services; (2) monitor their credit reports, financial accounts, and other records; and (3) take other steps to protect themselves and attempt to avoid or recover from identity theft.

102. Planned Parenthood was in a special relationship with Plaintiff and Class members as a result of being directly entrusted with their personal and highly sensitive medical information. Planned Parenthood holds itself out as "the most trusted provider of reproductive health care." Additionally, the end and aim of Defendant's data security measures was to benefit Plaintiff and Class members by ensuring that their personal information would remain protected and secure. Only Defendant was in a position to ensure that its systems were sufficiently secure to protect Plaintiff's and Class members' personal and medical information. The harm to Plaintiff and Class members from its exposure was highly foreseeable to Defendant.

103. The policy of preventing future harm disfavors application of the economic loss rule, particularly given the extreme sensitivity of the private information entrusted to Defendant. A high degree of opprobrium attaches to Defendant's failure to secure Plaintiff's and class members' personal and extremely confidential details. Defendant had an independent duty in tort to protect this information and thereby avoid reasonably foreseeable harm to Plaintiff and class members.

104. As a result of Defendant's negligence, Plaintiff and Class members have suffered damages that have included or may, in the future, include, without limitation: (1) loss of the opportunity to control how their personal information is used; (2)

diminution in the value and use of their personal information entrusted to Defendant with the understanding that Defendant would safeguard it against theft and not allow it to be accessed and misused by third parties; (3) the compromise and theft of their personal information; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft; (5) continued risk to their personal information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the personal information in its possession; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

FIFTH CAUSE OF ACTION

Invasion of Privacy

105. Plaintiff incorporates and realleges the foregoing allegations of fact.

106. Defendant wrongfully intruded upon Plaintiff's and Class members' seclusion. Plaintiff and Class members reasonably expected that the personal information they entrusted to Defendant, such as their full names, addresses, insurance information, dates of birth, and clinical information, such as diagnosis, procedure, and/or prescription information would be kept private and secure, and would not be disclosed to any unauthorized third party or for any improper purpose.

107. Defendant unlawfully invaded Plaintiff's and Class members' privacy rights by:

a. failing to adequately secure their personal information from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about them in a manner highly offensive to a reasonable person; and

c. enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

108. A reasonable person would find it highly offensive that Defendant, having

received, collected, and stored Plaintiff's and Class members' full names, addresses, insurance information, dates of birth, and clinical information, such as diagnosis, procedure, and/or prescription information and other highly sensitive personal details, failed to protect that information from unauthorized disclosure to third parties.

109. In failing to adequately protect Plaintiff's and Class members' personal information, Defendant acted knowingly and in reckless disregard of their privacy rights. Defendant knew of the security breaches experienced by other of its affiliates in the recent past. Defendant also knew or should have known that its ineffective security measures, and their foreseeable consequences, are highly offensive to a reasonable person in Plaintiff's position.

110. Defendant's unlawful invasions of privacy damaged Plaintiff and Class members. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiff and Class members suffered mental distress, and their reasonable expectations of privacy were frustrated and defeated. Accordingly, Plaintiffs and Class members are entitled to damages in an amount to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for an Order:

A. Certifying this case as a class action, appointing Plaintiff as Class representative, and appointing Plaintiff's counsel to represent the Class;

B. Entering judgment for Plaintiff and the Class;

C. Awarding Plaintiff and Class members monetary relief, including nominal damages;

D. Ordering appropriate injunctive or other equitable relief;

E. Awarding pre- and post-judgment interest as prescribed by law;

F. Awarding reasonable attorneys' fees and costs as permitted by law; and

G. Granting such further and other relief as may be just and proper.

REQUEST FOR JURY TRIAL

Plaintiff seeks a trial by jury on all issues so triable.

Dated: December 9, 2021

By: /s/ *Simon S. Grille*

Adam E. Polk (State Bar No. 273000)
Simon Grille (State Bar No. 294914)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
apolk@girardsharp.com
sgrille@girardsharp.com

Attorneys for Plaintiff and the Proposed Class