

1 Ronald A. Marron (175650)
 2 Alexis M. Wood (270200)
 3 Kas L. Gallucci (288709)
LAW OFFICES OF RONALD A. MARRON
 4 651 Arroyo Drive
 San Diego, CA 92103
 Telephone: (619) 696-9006
 5 Facsimile: (619) 564-6665
 ron@consumersadvocates.com
 alexis@consumersadvocates.com
 6 kas@consumersadvocates.com

7 Christian Levis (*pro hac forthcoming*)
 8 Amanda Fiorilla (*pro hac forthcoming*)
 Rachel Isabel Kesten (*pro hac vice forthcoming*)
LOWEY DANNENBERG, P.C.
 9 44 South Broadway, Suite 1100
 White Plains, NY 10601
 Telephone: (914) 997-0500
 10 Facsimile: (914) 997-0035
 11 clevis@lowey.com
 afiorilla@lowey.com
 12 rkesten@lowey.com

13 [*additional counsel on signature page*]

14 **IN THE UNITED STATES DISTRICT COURT**
 15 **FOR THE CENTRAL DISTRICT OF CALIFORNIA**

16 AMY PAWLUKIEWICZ, JACQUELINE
 17 DILANCHYAN, PAIGE MILLER,
 18 JAMILLAH DUNN, individually and on
 19 behalf of all others similarly situated,
 20
 Plaintiffs,
 21
 v.
 22
 23 PLANNED PARENTHOOD LOS
 ANGELES, a California nonprofit public
 24 benefit corporation, and PLANNED
 PARENTHOOD FEDERATION OF
 25 AMERICA, INC., a New York not-for-
 26 profit corporation,
 27
 Defendants.
 28

Case No.
CLASS ACTION COMPLAINT
JURY TRIAL DEMANDED

1 Plaintiffs Amy Pawlukiewicz, Jacqueline Dilanchyan, Paige Miller, and
2 Jamillah Dunn, on behalf of themselves and all others similarly situated, assert the
3 following against Defendants Planned Parenthood Los Angeles and Planned
4 Parenthood Federation of America, Inc. (collectively, “Planned Parenthood” or
5 “Defendants”) based upon personal knowledge, where applicable, information and
6 belief, and the investigation of counsel.

7 **INTRODUCTION**

8 1. Planned Parenthood Federation of America, Inc. (“PPFA”) proclaims
9 to be the nation’s leading provider of affordable health care for women, men, and
10 young people. PPFA provides a wide range of sexual and reproductive health care
11 to millions of people through a national network of more than 600 health centers
12 and clinics operated by their regional affiliates.

13 2. Planned Parenthood Los Angeles (“PPLA”) is a member-affiliate of
14 PPFA, and is one of the largest providers of comprehensive, reproductive health
15 care services in Los Angeles County.

16 3. In connection with its reproductive health care services, PPLA
17 promises to protect its patients’ health information and comply with any legal or
18 regulatory requirements.

19 4. For instance, PPLA promises that it “understand[s] that health
20 information about you and your health care is personal” such that it is “committed
21 to protecting health information about you.”¹ PPLA has a “pledge” in which it
22 promises to maintain the confidentiality of patients’ medical information that is
23 “backed-up by federal and state law.”

24 5. PPFA makes similar representations to patients, stating that it
25
26

27 ¹See Privacy Policy, Planned Parenthood Los Angeles,
28 <https://www.plannedparenthood.org/planned-parenthood-los-angeles/hipaa> (last
visited Dec. 8, 2021).

1 “respect[s] and [is] committed to protecting the privacy of users.”²

2 6. Given the extremely confidential and sensitive nature of the medical
3 services that Planned Parenthood provides to patients—and Planned Parenthood’s
4 representations—Plaintiffs and Class members reasonably expected that Planned
5 Parenthood’s data security practices complied with relevant laws, regulations, and
6 industry standards, and would be sufficient to protect the type of sensitive
7 information they collected and stored.

8 7. But these representations were false. Planned Parenthood did not
9 maintain adequate data security designed to protect the highly sensitive and
10 confidential nature of Plaintiffs’ and Class members’ personal and medical
11 information.

12 8. On October 17, 2021, PPLA identified suspicious activity on its
13 computer network. Despite knowing that its systems had been compromised since
14 mid-October, PPLA waited until November 30, 2021 to notify patients of the data
15 breach (the “Data Breach Notice Letter”). Attached hereto s **Exhibit A** is a copy
16 of the Data Breach Notice Letter transmitted to its patients.

17 9. The Data Breach Notice Letter explained that an “unauthorized
18 person” gained access to their network between October 9 – 17, 2021 (the “Breach
19 Period”). The unauthorized person “exfiltrated” files from their systems, including
20 patient names, dates of birth, addresses, and protected health information,
21 including insurance identification numbers, and clinical information, such as
22 diagnosis, treatment, or prescription information (collectively the “e-PHI”). The
23 data breach is estimated to have impacted approximately 400,000 patients.

24 10. The Data Breach Notice Letter downplayed the severity of the
25 intrusion and conveniently failed to notify patients that the data breach was caused

26 _____
27
28 ² See Privacy Policy, Planned Parenthood,
<https://www.plannedparenthood.org/privacy-policy> (last visited Dec. 8, 2021).

1 by *malware/ransomware*, which is a computer code *intentionally designed* to
2 infiltrate systems and gain access to private and sensitive information.

3 11. Instead, the Data Breach Notice Letter stated that there was “no
4 evidence that any information . . . has been used for fraudulent purposes” and that
5 patients were only being notified out of “an abundance of caution.” But these
6 assurances have no basis in fact, as PPLA cannot know what these hackers have
7 done (or intend to do) with Plaintiffs’ and Class members’ e-PHI once it was
8 exfiltrated from its systems. Indeed, PPLA contradicts its own statement by then
9 encouraging patients to “review statements you receive from your health insurer
10 and health care providers” given the risk of medical fraud that Plaintiffs and Class
11 members now face.

12 12. Doubling down on these omissions and misstatements, John M.
13 Erickson, a spokesman for PPLA, boldly stated there is “no indication this was a
14 targeted attack,” despite that the attack used malicious code designed explicitly for
15 this purpose.

16 13. Despite PPLA’s desire to downplay the severity of the data breach, it
17 has caused immediate, substantial harm to Plaintiffs and Class members.

18 14. Medical information, like the highly sensitive and confidential e-PHI
19 compromised here, is some of the most sensitive forms of personal information, as
20 it is immutable and cannot be changed. Planned Parenthood’s egregious handling
21 of this confidential and sensitive e-PHI, which is now in the hands of bad actors,
22 constitutes an extreme invasion of privacy. Patients consistently recognize the
23 importance of protecting medical information. A survey by the *Institute for Health*
24 *Freedom* found that 78% of patients feel it is “very important” that their medical
25 records be kept confidential. As a result of the data breach, Plaintiffs and Class
26 members no longer have control over their e-PHI, which is now forever in the
27 hands of bad actors.

28 15. Plaintiffs and Class members also have experienced emotional distress

1 as a result of the data breach because their e-PHI is now in the hands of bad actors
2 with illicit motives, such as publicly disclosing this information. Bad actors may
3 attempt to “dox” Plaintiffs and Class members, publishing their names, home
4 addresses, and reasons why they went to Planned Parenthood online. The threat of
5 this action in and of itself is emotionally distressing, as many of their friends, loved
6 ones, and family members may not be aware of their specific treatment at Planned
7 Parenthood. As a result of the data breach, they are constantly in a state of fear
8 and/or distress that this information may be made publicly available or extorted
9 against them.

10 16. Plaintiffs and Class members are now at an immediate risk of online
11 and even physical harassment, threats, intimidation, and retribution for visiting a
12 Planned Parenthood clinic, especially as their home addresses were disclosed in
13 connection with their sensitive medical information.

14 17. Anti-Planned Parenthood actors are known to target facilities, doctors,
15 and patients. In October 2020, a demonstration outside the Planned Parenthood
16 clinic in Walnut Creek, California took a violent turn when armed security guards
17 hired by anti-abortion activists pepper-sprayed counter protesters. The *National*
18 *Abortion Federation* (“NAF”) in their 2019 Violence and Disruption Statistics (the
19 most recent year statistics are available) found that internet harassment rose and
20 hate mail and harassing phone calls more than doubled with providers reporting
21 3,123 targeted incidents of hate mail and harassing phone calls, rising from 1,388
22 in 2018. According to the NAF, abortion care providers and staff continued to
23 receive focused threats through phone calls and text messages as well as postal
24 mail and flyers sent not only to health care facilities, but also to their homes. This
25 hate speech often escalates and turns into death threats and threats of harm.

26 18. As a result of the data breach, Plaintiffs and Class members have
27 suffered emotional distress, trauma, elevated stress, and anxiety, and remain in
28 constant fear of retaliation, harassment, and other acts of retribution.

1 19. Further, given the highly sensitive and confidential nature of the e-
2 PHI compromised by hackers in a malicious attack (i.e., through
3 malware/ransomware), Plaintiffs and Class members will be required to expend
4 significant time and effort to mitigate the effects of the data breach, such as
5 monitoring their credit reports and accounts for fraud.

6 20. This risk is ongoing because, unlike a credit card, there is no way to
7 cancel e-PHI. The U.S. Department of Health and Human Services (“HHS”) has
8 identified several imminent risks as a result of hackers obtaining patients’ e-PHI
9 including: (1) medical identity theft, i.e., the use of a patients’ medical information
10 to obtain medical services, such as medical prescriptions, surgery, or other medical
11 treatment, as well as counterfeit settlements against health insurers; (2) the
12 weaponization of medical data, i.e., the use of medical data to threaten, extort, or
13 influence the patient to extort money or disparage someone; (3) financial fraud,
14 i.e., the use of e-PHI to create credit card or bank accounts in the patients’ name,
15 taking out loans or lines of credit in the patients’ name, or the filing of fraudulent
16 tax documents or insurance information; and (4) cyber campaigns, using the
17 medical data in combination with other information on the dark web to commit
18 fraud, identity theft, conduct phishing or scams, or obtain the patients’ credentials
19 for other services. The “unauthorized person” who breached Planned Parenthood’s
20 systems can continue to exploit this information at the expense of Plaintiffs and the
21 Class. This ongoing imminent risk can often persist for years, as identity thieves
22 often hold stolen data for long periods of time before using it.

23 21. Such careless handling of e-PHI is prohibited by federal and state law.
24 For example, the Health Insurance Portability and Accountability Act of 1996
25 (“HIPAA”) requires healthcare providers, like Planned Parenthood, and their
26 business associates to safeguard patient e-PHI through a multifaceted approach that
27 includes, among other things: (a) ensuring the confidentiality, integrity, and
28 availability of all e-PHI they create, receive, maintain or transmit; (b) proactively

1 identifying and protecting against reasonably anticipated threats to the security or
2 integrity of e-PHI; (c) protecting against reasonably anticipated, impermissible
3 uses or disclosures of e-PHI; (d) putting in place the required administrative,
4 physical and technical safeguards to protect e-PHI; (e) implementing policies and
5 procedures to prevent, detect, contain, and correct security violations; (f)
6 effectively training their workforce regarding the proper handling of e-PHI; and (g)
7 designating individual security and privacy officers to ensure compliance with
8 these policies and procedures.

9 22. Planned Parenthood’s failure to comply with HIPAA and other laws
10 and/or guidelines as alleged herein by, among other things, failing to take
11 reasonable steps to safeguard patients’ highly sensitive and confidential e-PHI, has
12 directly resulted in injury to Plaintiffs and the Class.

13 23. Given the secret nature of, among other things: (a) Planned
14 Parenthood’s policies, procedures, systems, and controls; (b) the result of the
15 “investigation” into the data breach disclosed in the Data Breach Notice Letter; and
16 (c) communications among Planned Parenthood and/or the “third-party
17 cybersecurity firm [who] was engaged to assist in [their] investigation” concerning
18 the data breach referenced in the Data Breach Notice Letter, Plaintiffs believe that
19 further evidentiary support for their claims will be unearthed after a reasonable
20 opportunity for discovery.

21 24. Plaintiffs and Class members bring claims for invasion of their
22 privacy interests, as established through California’s privacy laws and California’s
23 Constitution. In addition, Planned Parenthood’s actions constitute negligence,
24 breach of contract and implied contract, unjust enrichment, as well as violations of
25 several state consumer protection and privacy laws.

26 25. Plaintiffs seek to remedy these harms on behalf of themselves and all
27 similarly situated individuals whose highly sensitive and confidential e-PHI was
28 stolen in the data breach. Plaintiffs and Class members seek remedies including but

1 not limited to statutory damages, compensatory damages, and injunctive relief
2 requiring substantial improvements to Planned Parenthood’s security systems.

3 **PARTIES**

4 **I. PLAINTIFFS**

5 26. Plaintiff **Amy Pawlukiewicz** (“Plainiff Pawlukiewicz”) is a natural
6 person and citizen of the State of California and a resident of Los Angeles County.
7 Plaintiff Pawlukiewicz received medical treatment at the Planned Parenthood Los
8 Angeles Canoga Park clinic for women’s healthcare services in 2020 and paid for
9 services

10 27. Plaintiff Pawlukiewicz provided Planned Parenthood with her highly
11 sensitive and confidential e-PHI, including her name, date of birth, address,
12 insurance information, and medical history. Records reflecting Plaintiff
13 Pawlukiewicz’s treatment contained additional personal and highly sensitive e-
14 PHI, including the reason(s) for her visit and treatment information. This
15 information, along with other e-PHI associated with Plaintiff Pawlukiewicz’s
16 treatment was stored electronically on Planned Parenthood’s servers during the
17 Breach Period and as described below, was accessed and exfiltrated without her
18 consent.

19 28. On or about November 30, 2021, Planned Parenthood Los Angeles
20 notified Plaintiff Pawlukiewicz that her highly sensitive and confidential e-PHI
21 was compromised as a result of the data breach.

22 29. Given that Plaintiff Pawlukiewicz’s highly sensitive and confidential
23 e-PHI was accessed and exfiltrated without her consent as a result of the data
24 breach, Plaintiff Pawlukiewicz has suffered concrete harm, including: (1) the
25 unauthorized disclosure of her private health information to third parties; (2) the
26 imminent risk of fraud and identity theft; (3) the intrusion upon seclusion and
27 violation of her reasonable expectation of privacy in such highly sensitive medical
28 information, such as that related to her medical history and treatment; (4) and the

1 increased risk of the threat of online and physical harassment and retribution for
2 utilizing Planned Parenthood’s reproductive health care services; and (5) emotional
3 distress.

4 30. Plaintiff **Jacqueline Dilanchyan** (“Plaintiff Dilanchyan”) is a natural
5 person and citizen of the State of California and a resident of Los Angeles County.
6 Plaintiff Dilanchyan received medical treatment at the Planned Parenthood Los
7 Angeles Burbank clinic for women’s healthcare services in 2018 and paid for
8 services.

9 31. Plaintiff Dilanchyan provided Planned Parenthood with her highly
10 sensitive and confidential e-PHI, including her name, date of birth, address,
11 insurance information, and medical history. Records reflecting Plaintiff
12 Dilanchyan’s treatment contained additional personal and highly sensitive e-PHI,
13 including the reason(s) for her visit and treatment information. This information,
14 along with other e-PHI associated with Plaintiff Dilanchyan’s treatment was stored
15 electronically on Planned Parenthood’s servers during the Breach Period and as
16 described below, was accessed and exfiltrated without her consent.

17 32. On or about November 30, 2021, Planned Parenthood Los Angeles
18 notified Plaintiff Dilanchyan that her highly sensitive and confidential e-PHI was
19 compromised as a result of the data breach.

20 33. Given that Plaintiff Dilanchyan’s highly sensitive and confidential e-
21 PHI was accessed and exfiltrated without her consent as a result of the data breach,
22 Plaintiff Dilanchyan has suffered concrete harm, including: (1) the unauthorized
23 disclosure of her private health information to third parties; (2) the imminent risk
24 of fraud and identity theft; (3) the intrusion upon seclusion and violation of her
25 reasonable expectation of privacy in such highly sensitive medical information,
26 such as that related to her medical history and treatment; (4) and the increased risk
27 of the threat of online and physical harassment and retribution for utilizing Planned
28 Parenthood’s reproductive health care services; and (5) emotional distress.

1 34. Plaintiff **Paige Miller** (“Plaintiff Miller”) is a natural person and
2 citizen of the State of California and a resident of Los Angeles County. Plaintiff
3 Miller received medical treatment at the Planned Parenthood Los Angeles
4 Lawndale clinic for women’s healthcare services several times since 2018.

5 35. Plaintiff Miller provided Planned Parenthood with her highly sensitive
6 and confidential e-PHI, including her name, date of birth, address, insurance
7 information, and medical history. Records reflecting Plaintiff Miller’s treatment
8 contained additional personal and highly sensitive e-PHI, including the reason(s)
9 for her visit and treatment information. This information, along with other e-PHI
10 associated with Plaintiff Miller’s treatment was stored electronically on Planned
11 Parenthood’s servers during the Breach Period and as described below, was
12 accessed and exfiltrated without her consent.

13 36. On or about November 30, 2021, Planned Parenthood Los Angeles
14 notified Plaintiff Miller that her highly sensitive and confidential e-PHI was
15 compromised as a result of the data breach.

16 37. Given that Plaintiff Miller’s highly sensitive and confidential e-PHI
17 was accessed and exfiltrated without her consent as a result of the data breach,
18 Plaintiff Miller has suffered concrete harm, including: (1) the unauthorized
19 disclosure of her private health information to third parties; (2) the imminent risk
20 of fraud and identity theft; (3) the intrusion upon seclusion and violation of her
21 reasonable expectation of privacy in such highly sensitive medical information,
22 such as that related to her medical history and treatment; (4) and the increased risk
23 of the threat of online and physical harassment and retribution for utilizing Planned
24 Parenthood’s reproductive health care services; and (5) emotional distress.

25 38. Plaintiff **Jamillah Dunn** (“Plaintiff Dunn”) is a natural person and
26 citizen of the State of California and a resident of Los Angeles County. Plaintiff
27 Dunn received medical treatment at the Planned Parenthood Los Angeles La Brea,
28 West Hollywood and Los Angeles clinics for women’s healthcare services several

1 times for over twenty-five years.

2 39. Plaintiff Dunn provided Planned Parenthood with her highly sensitive
3 and confidential e-PHI, including her name, date of birth, address, insurance
4 information, and medical history. Records reflecting Plaintiff Dunn’s treatment
5 contained additional personal and highly sensitive e-PHI, including the reason(s)
6 for her visit and treatment information. This information, along with other e-PHI
7 associated with Plaintiff Dunn’s treatment was stored electronically on Planned
8 Parenthood’s servers during the Breach Period and as described below, was
9 accessed and exfiltrated without her consent.

10 40. On or about November 30, 2021, Planned Parenthood Los Angeles
11 notified Plaintiff Dunn that her highly sensitive and confidential e-PHI was
12 compromised as a result of the data breach.

13 41. Given that Plaintiff Dunn’s highly sensitive and confidential e-PHI
14 was accessed and exfiltrated without her consent as a result of the data breach,
15 Plaintiff Dunn has suffered concrete harm, including: (1) the unauthorized
16 disclosure of her private health information to third parties; (2) the imminent risk
17 of fraud and identity theft; (3) the intrusion upon seclusion and violation of her
18 reasonable expectation of privacy in such highly sensitive medical information,
19 such as that related to her medical history and treatment; (4) and the increased risk
20 of the threat of online and physical harassment and retribution for utilizing Planned
21 Parenthood’s reproductive health care services; and (5) emotional distress.

22 **II. DEFENDANTS**

23 **A. PPFA**

24 42. Defendant **Planned Parenthood Federation of America, Inc.**
25 (“PPFA”) is a New York not-for-profit corporation with principal executive offices
26 located at 123 William Street, New York, NY 10038.

27 43. PPFA is the leading national organization dedicated to offering
28 affordable health care services, public education, and advocacy in the field of

1 reproductive health care. PPFA’s core mission is to ensure the provision of high-
2 quality, non-judgmental comprehensive reproductive health care services, to
3 provide educational programs relating to reproductive and sexual health, and to
4 advocate for public policies to ensure access to health services—including for
5 individuals with low incomes or from underserved communities. PPFA also
6 engages in public education about, and advocacy in favor of, the right to access
7 safe and legal abortions.

8 44. PPFA is a membership organization composed of more than fifty
9 affiliate organizations, with a Board of Directors. The member-affiliates are
10 responsible for setting the long-range goals and priorities of PPFA and for electing
11 the PPFA Board of Directors. Through their participation and voting, PPFA’s
12 member-affiliates control the mission and direction of PPFA. Historically PPFA’s
13 member affiliates were required to contribute financially to PPFA. Each affiliate of
14 PPFA has the right to use the Planned Parenthood name and service mark.

15 45. Cumulatively, PPFA’s member-affiliates operate more than 600
16 health centers that provide a wide range of reproductive health care services and
17 education. Among them are contraception (including long-acting reversible
18 contraceptives (“LARCs”)), contraceptive counseling, physical exams, clinical
19 breast exams, screening for cervical and testicular cancers, testing and treatment
20 for sexually transmitted infections (“STIs”), treatment of sexual dysfunction in
21 men, pregnancy testing and counseling, pre-natal care, testing and treatment for
22 HIV, gender affirming care including hormone therapy for transgender patients,
23 some sterilization services (including vasectomies), colposcopies, abortion, and
24 health education services. PPFA’s affiliates also provide referrals for these services
25 if they are unable to provide them at their health centers.

26 46. In 2019, Planned Parenthood affiliates provided more than 10.4
27 million services to approximately 2.4 million patients. Planned Parenthood
28 affiliates provided more than 5.4 million STI testing and treatment services, more

1 than 2.5 million contraceptive services, administered more than 598,000 cancer
2 screenings and preventive services such as breast exams and cervical screens (Pap
3 tests), conducted more than 860,000 HIV tests, and performed more than 350,000
4 abortions.

5 47. An estimated one out of every three women nationally has received
6 care from a Planned Parenthood affiliate at least once in her life.

7 **B. PPLA**

8 48. Defendant **Planned Parenthood Los Angeles** (“PPLA”) is a
9 California nonprofit public benefit corporation with principal executive offices
10 located at 400 W. 30th Street, Los Angeles, CA 90007.

11 49. PPLA is a member-affiliate of PPFA. PPLA utilizes the Planned
12 Parenthood name and service mark on its website, messaging, and
13 communications, including on the Data Breach Notice Letter sent to Plaintiffs and
14 the Class. In addition, the CEO of PPLA, Susan Dunlap, is a member of PPFA’s
15 Board of Directors.

16 50. According to PPLA, its mission “is to provide convenient and
17 affordable access to a comprehensive range of quality reproductive health care and
18 sexual health information through patient services, education and advocacy.”

19 51. PPLA is one of the largest providers of comprehensive, reproductive
20 health care services in Los Angeles County. PPLA’s reproductive health care
21 services include but are not limited to, pregnancy testing and services, STI testing
22 and treatment, contraception services, abortion and emergency contraception, as
23 well as general men’s, women’s, and LGBT health care services.

24 52. PPLA operates twenty-one California (21) health centers. Of the
25 women, men, and young people who rely on PPLA for care, 84% receive family
26 planning services and 78% are living at or below the federal poverty level.

27 53. PPLA represents that “Planned Parenthood providers are among the
28 best-trained and most experienced in the field of reproductive health care” and that

1 it “offer[s] a level of nonjudgmental care that’s hard to find anywhere else.”
2 Further, PPLA pledges to protect its patients’ health information and comply with
3 any legal or regulatory requirements. PPLA states that it “understand[s] that health
4 information about you and your health care is personal” such that it is “committed
5 to protecting health information about you.” PPLA’s pledge promises to maintain
6 the confidentiality of patients’ medical information that is “backed-up by federal
7 and state law.” However, despite this pledge, PPLA failed to secure its patients
8 highly sensitive and confidential e-PHI, which has been exfiltrated which was seen
9 by unauthorized third parties and can now be weaponized and used to harass and
10 threaten the patients who used its services.

11 54. Upon information and belief, PPLA and PPFA share common servers,
12 networks, systems, databases, and/or healthcare and patient management systems.

13 55. PPLA and PPFA are collectively referred to throughout the Complaint
14 as “Planned Parenthood” or “Defendants.”

15 **JURISDICTION AND VENUE**

16 56. This Court has jurisdiction over the subject matter of this action
17 pursuant to 28 U.S.C § 1332(d), because there are more than 100 putative members
18 of the Classes, as defined below, a significant portion of putative Class members
19 are citizens of a state different from Defendants, and the amount in controversy for
20 the Classes exceeds \$5,000,000 exclusive of interest and costs. Given the estimated
21 size of the class (i.e., approximately 400,000 patients), statutory damages available
22 to Plaintiffs and Class members under the CMIA far exceed the \$5 million
23 threshold. As does the likely value of any injunctive relief, including changes to
24 Planned Parenthood’s systems and procedures to prevent future data breaches, and
25 the value of Plaintiffs’ and Class members’ right to seclusion and non-disclosure of
26
27
28

1 their confidential and sensitive e-PHI.³

2 57. This Court has personal jurisdiction over PPLA because PPLA
3 maintains its principal executive offices in Los Angeles, California and is a
4 registered California corporation.

5 58. This Court has personal jurisdiction over PPFA because PPFA has
6 sufficient minimum contacts in California. For example, PPFA purposefully
7 availed itself of the privileges and benefits associated with conducting business in
8 this state, by, among other things, reaching into California to establish an affiliated
9 partnership with its PPFA member-affiliate—PPLA. Under PPFA’s bylaws,
10 historically PPFA’s member-affiliates, including PPLA are also required to
11 contribute financially to PPFA, and affiliate dues contribute to PPFA’s financial
12 support. PPFA allows its affiliates, including PPLA the right to use the Planned
13 Parenthood name and service mark in California, which PPLA displays on its
14 website. Further, upon information and belief, PPFA shares common servers,
15 networks, systems, databases, and/or healthcare and patient management systems
16 with PPLA.

17 59. Venue is proper in this District pursuant to 28 U.S.C. §1391(b)(2)
18 because Defendants transact business in this District and a substantial portion of
19 the events giving rise to the claims occurred in this District.

20
21
22
23
24
25
26
27
28

³ For purposes of this Complaint, Plaintiffs estimate the value of these rights to be worth at least \$10 million by multiplying the average cost to protect against such a breach using identity theft insurance (approximately \$25 to \$60 per person, per year) by the approximately 400,000 persons whose e-PHI was accessed without consent. Plaintiffs reserve their rights to revise or supplement this estimate following a reasonable opportunity for discovery.

FACTUAL BACKGROUND

III. THE PLANNED PARENTHOOD DATA BREACH

60. In connection with its services, PPLA has consistently promised patients that it pledges to protect its patients’ health information and comply with any legal or regulatory requirements. For instance, PPLA promises that it “understand[s] that health information about you and your health care is personal” such that it is “committed to protecting health information about you.”⁴ As part of PPLA’s “pledge,” it promises to maintain the confidentiality of patients’ medical information and that it is “backed-up by federal and state law.”

61. PPLA has dedicated a section on its website to apprise its patients, including Plaintiffs and Class members, of the permissible uses and disclosure of their medical records.

62. More specifically, PPLA posts on its website a “HIPAA Privacy Policy | NOTICE OF HEALTH INFORMATION PRIVACY PRACTICES” dated September 1, 2014 (the “Privacy Policy”), which PPLA admits they are required to comply with. In its Privacy Policy, PPLA pledges to protect its patients’ health information and states “[w]e understand that health information about you and your health care is personal. We are committed to protecting health information about you.”

63. Specifically, PPLA’s “pledge” states “[o]ur pledge regarding your health information is backed-up by federal and state law. The privacy and security provisions of the federal Health Insurance Portability and Accountability Act (“HIPAA”) require us to: Make sure that health information that identifies you is kept private; Make available this notice of our legal duties and privacy practices with respect to health information about you; and Follow the terms of the notice

⁴ See Privacy Policy Planned Parenthood Los Angeles, <https://www.plannedparenthood.org/planned-parenthood-los-angeles/hipaa> (last visited Dec. 8, 2021).

1 that is currently in effect.”

2 64. These promises were false. As a result of Planned Parenthood’s
3 deficient data security, between October 9 – 17, 2021, unauthorized third parties
4 using malicious code, i.e., malware and ransomware, gained access and exfiltrated
5 Plaintiffs’ and Class members’ highly sensitive and confidential e-PHI. As a result,
6 these unauthorized third parties have seen Plaintiffs’ and Class members highly
7 sensitive and confidential e-PHI.

8 65. Week a month later, on November 30, 2021, PPLA finally notified
9 patients, including Plaintiffs, of the data breach and that their highly sensitive and
10 confidential e-PHI was compromised.

11 66. PPLA determined that the “unauthorized person” installed
12 malware/ransomware to gain access to its network and exfiltrated files from its
13 systems. Ransomware is a malicious computer code intentionally designed to block
14 an organization’s access to its own computer network to extort a ransom. Malware
15 is malicious computer code explicitly designed to exfiltrate files or otherwise cause
16 harm to computer networks.

17 67. PPLA determined that the files exfiltrated by bad actors included
18 patients’ names, and one or more of the following: dates of birth, addresses, and
19 protected health information including insurance identification numbers, and
20 clinical data, such as diagnosis, treatment, or prescription information.

21 68. While PPLA’s “Notice of Patient Privacy Incident” included on its
22 website indicates that the unauthorized person “installed malware/ransomware and
23 exfiltrated some files from our systems,” PPLA’s Data Breach Notice Letter to
24 Plaintiffs downplays the intrusion and fails to include the relevant information that
25 malware/ransomware was installed. This is especially problematic as malware and
26 ransomware are notoriously used by bad actors with malintent.

27 69. The cyber criminals who committed the data breach viewed, obtained,
28 and exfiltrated Plaintiffs’ and Class members’ highly sensitive and confidential e-

1 PHI for malicious purposes and now have it available to them to sell to other bad
2 actors or otherwise misuse the information, including “doxing” Plaintiffs and Class
3 members. This “doxing” can include publishing their names, home addresses, and
4 reasons why they went to Planned Parenthood online.

5 70. Significantly, Planned Parenthood does not represent that Plaintiffs’
6 and Class members’ e-PHI was encrypted, password protected, or secured in some
7 other manner that would prevent the malicious actors from actually using the
8 information. Upon information and belief, these malicious actors who gained
9 Plaintiffs’ and Class members’ e-PHI now have unfettered access.

10 **IV. PLANNED PARENTHOOD’S HISTORY OF DATA BREACHES**

11 71. This is not the first time PPFA, or its affiliates experienced a data
12 breach as a result of their severely deficient data security. PPFA and its affiliates
13 have been the target of hackers and anti-abortion groups for many years because of
14 its status as a prominent nationally recognized organization that advocates for
15 reproductive rights.

16 72. In July 2015, PPFA was targeted by a group of hackers called “3301”
17 who gained access to the names and contact information, including email addresses
18 and passwords, of hundreds of PPFA employees across the nation. The 3301
19 hackers also planned to deface the PPFA website and “dump” multiple of their
20 databases, i.e., expose it to the public. The 3301 hackers then exposed the users’
21 usernames, emails, and passwords.

22 73. In 2020, PPFA’s software vendor, Blackbaud, Inc., experienced a data
23 breach between February 7 and May 20, 2020 that compromised the personal
24 information of donors of several affiliated Planned Parenthoods. The perpetrators
25 of that attack held the data for ransom.

26 74. Most recently, on April 9, 2021, PPFA member-affiliate Planned
27 Parenthood of Metropolitan Washington D.C., revealed that it suffered a data
28 breach between August 27, 2020 and October 8, 2020, whereby unauthorized

1 actors gained access to their network and acquired patient and donor data for an
2 undisclosed number of people. The data compromised included names, addresses,
3 dates of birth, diagnoses, treatments, prescription information, social security
4 numbers, and financial information. Additionally, among the leaked documents
5 were check images with donor's names, bank account, and routing numbers. In
6 addition to patient information, the leaked donor information provided those bad
7 actors additional ammunition to weaponize the leaked data as it exposed those who
8 had contributed to reproductive rights causes as targets for harassment and
9 intimidation.

10 75. Given the numerous instances in which Planned Parenthood has failed
11 to protect patients and employees, it was on notice that its data security systems
12 were deficient. Despite this, Planned Parenthood has continued to maintain
13 woefully deficient data security, which resulted in Plaintiffs' and Class members'
14 highly sensitive and confidential e-PHI being compromised by bad actors.

15 **V. PLANNED PARENTHOOD FAILED TO COMPLY WITH HIPAA,**
16 **THE NATIONAL STANDARD FOR PROTECTING PRIVATE**
17 **HEALTH INFORMATION**

18 76. HIPAA requires the healthcare industry to have a generally accepted
19 set of security standards for protecting health information. HIPAA defines
20 Protected Health Information ("PHI") as individually identifiable health
21 information and e-PHI that is transmitted by electronic media or maintained in
22 electronic media. This protected information includes: names, dates, phone
23 numbers, fax numbers, email addresses, SSNs, medical record numbers, health
24 insurance beneficiary numbers, account numbers, certificate/license numbers,
25 vehicle identifiers, device identifiers and serial numbers, URLs, IP addresses,
26 biometric identifiers, photographs, and any other unique identifying number,
27 characteristic, or code.

28 77. To this end, HHS promulgated the HIPAA Privacy Rule in 2000 and

1 the HIPAA Security Rule in 2003. The security standards for the protection of e-
2 PHI, known as “the Security Rule,” establish a national set of security standards
3 for protecting certain health information that is held or transferred in electronic
4 form. The Security Rule operationalizes the protections contained in the Privacy
5 Rule by addressing the technical and non-technical safeguards that organizations
6 called “covered entities” must put in place to secure individuals’ e-PHI.

7 78. Defendants are either an entity covered by HIPAA, *see* 45 C.F.R. §
8 160.102, or “business associates” covered by HIPAA, *see* 45 C.F.R. § 160.103,
9 and therefore must comply with the HIPAA Privacy Rule and Security Rule, *see*
10 45 C.F.R. Part 160 and Part 164, Subparts A, C, and E.

11 79. HIPAA limits the permissible uses of e-PHI and prohibits the
12 unauthorized disclosure of e-PHI. *See* 45 C.F.R. § 164.502. HIPAA also requires
13 that covered entities implement appropriate safeguards to protect this information.
14 *See* 45 C.F.R. § 164.530(c)(1).

15 80. The electronically stored healthcare information accessed by
16 unauthorized third parties on Planned Parenthood’s servers are e-PHI under the
17 HIPAA Privacy Rule and the Security Rule, which protects all e-PHI a covered
18 entity “creates, receives, maintains or transmits” in electronic form. 45 C.F.R. §
19 160.103.

20 81. The Security Rule requires covered entities, including Planned
21 Parenthood, to implement and maintain appropriate administrative, technical, and
22 physical safeguards for protecting e-PHI. *See* 45 C.F.R. § 164.530(c)(1). Among
23 other things, the Security Rule requires Planned Parenthood to identify and
24 “[p]rotect against any reasonably anticipated threats or hazards to the security or
25 integrity of [the] information” and “[p]rotect against any reasonably anticipated
26 uses or disclosures.” 45 C.F.R. § 164.306.

27 82. HIPAA also obligates Planned Parenthood to implement policies and
28 procedures to prevent, detect, contain, and correct security violations. *See* 45

1 C.F.R. § 164.308(a)(1)(i).

2 83. HIPAA further obligates Planned Parenthood to ensure that their
3 workforce comply with HIPAA security standard rules, *see* 45 C.F.R. §
4 164.306(a)(4), to effectively train their workforces on the policies and procedures
5 with respect to protected health information, as necessary and appropriate for those
6 individuals to carry out their functions and maintain the security of protected
7 health information. *See* 45 C.F.R. § 164.530(b)(1).

8 84. Planned Parenthood failed to comply with these HIPAA rules.
9 Specifically, Planned Parenthood failed to put in place the necessary technical and
10 non-technical safeguards required to protect Plaintiffs’ and Class members’ highly
11 sensitive and confidential e-PHI.

12 **VI. PLANNED PARENTHOOD VIOLATED THE FTC ACT**

13 85. Planned Parenthood was (and still is) prohibited from engaging in
14 “unfair or deceptive acts or practices in or affecting commerce” by the Federal
15 Trade Commission Act, 15 U.S.C. § 45. Their failure to employ reasonable and
16 appropriate measures to protect against unauthorized access to confidential
17 consumer data constitutes an unfair act or practice that violates this rule.

18 86. In 2007, the FTC published guidelines establishing reasonable data
19 security practices for businesses. The guidelines note that businesses should protect
20 the personal customer information that they keep; properly dispose of personal
21 information that is no longer needed; encrypt information stored on computer
22 networks; understand their network’s vulnerabilities; and implement policies for
23 installing vendor-approved patches to correct security problems. The guidelines
24 also recommend that businesses consider using an intrusion detection system to
25 expose a breach as soon as it occurs; monitor all incoming traffic for activity
26 indicating someone may be trying to hack the system; watch for large amounts of
27 data being transmitted from the system; and have a response plan ready in the
28 event of a breach.

1 87. The FTC has also published a document entitled “FTC Facts for
2 Business,” which highlights the importance of having a data security plan,
3 regularly assessing risks to computer systems, and implementing safeguards to
4 control such risks.

5 88. Planned Parenthood was aware of and failed to follow the FTC
6 guidelines and failed to adequately secure patients’ data stored on their servers.
7 Furthermore, by failing to have reasonable data security measures in place,
8 Planned Parenthood engaged in an unfair act or practice within the meaning of § 5
9 of the FTC Act.

10 89. In addition to the FTC Act, Planned Parenthood had a duty to adopt
11 reasonable data security measures in accordance with federal law under HIPAA as
12 well as the laws of the various states in which it operates, including the CMIA

13 **VII. PLANNED PARENTHOOD VIOLATED THEIR COMMON LAW**
14 **DUTY OF REASONABLE CARE**

15 90. In addition to obligations imposed by federal and state law, Planned
16 Parenthood owed and continues to owe a common law duty to Plaintiffs and Class
17 members—who entrusted Planned Parenthood with their highly sensitive and
18 confidential e-PHI—to exercise reasonable care in receiving, maintaining, storing,
19 and deleting the e-PHI in Planned Parenthood’s possession.

20 91. Planned Parenthood owed and continues to owe a duty to prevent
21 Plaintiffs’ and Class members’ highly sensitive and confidential e-PHI from being
22 compromised, lost, stolen, accessed, or misused by unauthorized third parties. An
23 essential part of Planned Parenthood’s duty was (and is) the obligation to provide
24 reasonable security consistent with current industry best practices and
25 requirements, and to ensure information technology systems and networks, in
26 addition to the personnel responsible for those systems and networks, adequately
27 protected and continue to protect Plaintiffs’ and Class members’ highly sensitive
28 and confidential e-PHI.

1 92. Planned Parenthood owed a duty to Plaintiffs and Class members,
2 who entrusted Planned Parenthood with their highly sensitive and confidential e-
3 PHI, to design, maintain, and test the information technology systems that housed
4 Plaintiffs’ and Class members’ highly sensitive and confidential e-PHI, to ensure
5 that the highly sensitive and confidential e-PHI in Planned Parenthood’s
6 possession was adequately secured and protected.

7 93. Planned Parenthood owed a duty to Plaintiffs and Class members to
8 create, implement, and maintain reasonable data security practices and procedures
9 sufficient to protect the highly sensitive and confidential e-PHI stored in Planned
10 Parenthood’s computer systems. This duty required Planned Parenthood to
11 adequately train employees and others with access to Plaintiffs’ and Class
12 members’ highly sensitive and confidential e-PHI on the procedures and practices
13 necessary to safeguard such sensitive information.

14 94. Planned Parenthood owed a duty to Plaintiffs and Class members to
15 implement processes that would enable Planned Parenthood to timely detect a
16 breach of its information technology systems, and a duty to act upon any data
17 security warnings or red flags detected by such systems in a timely fashion.

18 95. Planned Parenthood owed a duty to Plaintiffs and Class members to
19 disclose when and if Planned Parenthood’s information technology systems and
20 data security practices were not sufficiently adequate to protect and safeguard
21 Plaintiffs’ and Class members’ highly sensitive and confidential e-PHI.

22 96. Planned Parenthood violated these duties. Planned Parenthood did not
23 implement measures designed to timely detect a breach of their information
24 technology systems, as required to adequately safeguard Plaintiffs’ and Class
25 members’ highly sensitive and confidential e-PHI. Planned Parenthood also
26 violated their duty to create, implement, and maintain reasonable data security
27 practices and procedures sufficient to protect Plaintiffs’ and Class members’ highly
28 sensitive and confidential e-PHI. As the Data Breach Notice Letter states, “a third-

1 party cybersecurity firm was engaged to assist in our investigation,” *after the*
2 *breach* occurred. Planned Parenthood should have taken these steps *beforehand* to
3 protect the highly sensitive and confidential e-PHI in their possession and prevent
4 the breach from occurring, as required under HIPAA and FTC guidelines, as well
5 as other state and federal law and/or regulations.

6 97. Planned Parenthood owed a duty to Plaintiffs and Class members to
7 timely disclose the fact that a data breach, resulting in unauthorized access to their
8 highly sensitive and confidential e-PHI, had occurred.

9 **VIII. PLANNED PARENTHOOD FAILED TO COMPLY WITH THEIR**
10 **OWN PRIVACY POLICY AND OTHER REPRESENTATIONS**

11 98. PPLA’s Privacy Policy lists the permitted uses and disclosures of
12 patients’ highly sensitive and confidential e-PHI and informs patients that e-PHI
13 will be used for: (i) treatment; (ii) payment; (iii) healthcare operations; (iv)
14 appointment reminders; (v) to individuals involved in their care or payment for
15 their care; (vi) research; (vii) fundraising activities; (viii) as required by law; (ix) to
16 avert a serious threat to health or safety; (x) military and veterans; (xi) workers’
17 compensation; (xii) public health risks; (xiii) health oversight activities; (xiv)
18 lawsuits and disputes; (xv) law enforcement; (xvi) inmates; and (xvii) coroners,
19 health examiners and funeral directors.

20 99. PPLA’s Privacy Policy further states that the “following uses and
21 disclosures of health information will be made only with your written permission:
22 [u]ses and disclosures of protected health information for marketing purposes;
23 [u]ses and disclosures that constitute the sale of your protected health information;
24 [and] [o]ther uses and disclosures of health information not covered by this Notice
25 or the laws that apply to us.”

26 100. Critically, none of the permissible uses in PPLA’s Privacy Policy of e-
27 PHI include granting unfettered access to unauthorized third parties who intend to
28 misuse such information for illicit purposes.

1 101. PPLA’s Privacy Policy further assuages patients’ concerns regarding
2 unauthorized disclosure of their personal information by allowing them to revoke
3 any written authorizations: “[i]f you provide us permission to use or disclose health
4 information about you, you may revoke that permission, in writing, at any time. If
5 you revoke your permission, we will no longer use or disclose health information
6 about you for the reasons covered by your written authorization.”

7 102. By these representations in the Privacy Policy, PPLA affirmatively—
8 and misleadingly—assured patients, including Plaintiffs and the Class members,
9 that they had the ability to control the dissemination of their highly sensitive and
10 confidential e-PHI and to restrict its use and access by third parties.

11 103. The Privacy Policy also expressly guaranteed PPLA would safeguard
12 patients’ highly sensitive and confidential e-PHI consistent with the applicable
13 laws and regulations.

14 104. However, PPLA failed to safeguard patients’ highly sensitive and
15 confidential e-PHI in violation of their own Privacy Policy and applicable law and
16 regulations, as confirmed by the Notice of Patient Privacy Incident, in which PPLA
17 admits that an “unauthorized person gained access to our network between October
18 9, 2021 and October 17, 2021, installed malware/ransomware and exfiltrated some
19 files from our systems during that time.” In fact, PPLA failed to take any steps to
20 safeguard Plaintiffs’ and Class members’ highly sensitive and confidential e-PHI
21 until after the data breach occurred.

22 105. PPLA failure to implement appropriate security measures and
23 adequately safeguard Plaintiffs’ and Class members’ highly sensitive and
24 confidential e-PHI violated the terms of their own Privacy Policy and other
25 representations.

26
27
28

1 **IX. THE DATA BREACH DAMAGES PLAINTIFFS AND CLASS**
2 **MEMBERS**

3 106. As a result of Planned Parenthood’s deficient security measures,
4 Plaintiffs and Class members have been harmed by the compromise of their highly
5 sensitive and confidential e-PHI.

6 107. Several criminal syndicates, including Ukraine’s UNC1878 and
7 China’s Dynamite Panda, along with various state-sponsored groups, are known to
8 target hospitals and healthcare providers based on the high value associated with e-
9 PHI, both as a revenue stream (e.g., when sold on the dark web, or used to commit
10 identify theft) and as a tool for executing future hacks (e.g., by impersonating users
11 or providing information that can be useful in cracking passwords or security
12 questions). Plaintiffs reasonably anticipate that the identity of the hackers involved
13 in the data breach will be revealed in discovery.

14 108. This exfiltrated highly sensitive and confidential e-PHI can be used
15 for malicious purposes, including doxing, harassment, financial fraud, medical
16 identity theft, identity theft, insurance fraud, and crafting convincing phishing
17 messages. Plaintiffs and Class members face an imminent risk of:

- 18 a. *medical identity theft*—the use of another person’s medical
19 information to obtain a medical service;
- 20 b. *weaponizing of medical data*—the use of sensitive medical data
21 to threaten, harass, extort, or influence individuals;
- 22 c. *financial fraud*—the use of personally identifiable information
23 contained in medical records to create credit card or bank or
24 insurance profiles to facilitate financial and insurance fraud;
25 and,
- 26 d. *cyber campaigns*—the use of medical data as complementary
27 data in future hacking campaigns.

28 109. As a result, e-PHI has become increasingly valuable on the black
market. In fact, it is more valuable than any other type of record on the dark web.

1 For example, according to *Forbes*, as of April 14, 2017, the going rate for an SSN
2 is \$.010 cents and a credit card number is worth \$.025 cents, but medical records
3 containing e-PHI could be worth hundreds or even thousands of dollars. For
4 example, in April of 2019, HHS estimated that the average price of medical
5 records containing e-PHI ranged between \$250 and \$1,000.

6 110. The Fifth Annual Study on Medical Identity Theft conducted by the
7 *Ponemon Institute* concluded that medical identity theft alone costs the average
8 victim \$13,500 to fix.

9 111. According to *The World Privacy Forum*, a nonprofit public interest
10 group, one of the reasons for this price differential is that criminals are able to
11 extract larger illicit profits using medical records than they are for a credit card or
12 SSN. For example, while a credit card or SSN typically yields around \$2,000
13 before being canceled or changed, an individual's e-PHI typically yields \$20,000
14 or more. This is because, in addition to the fact that healthcare data and e-PHI are
15 immutable (e.g., you cannot cancel your medical records), healthcare data breaches
16 often take much longer to be discovered, allowing thieves to leverage e-PHI for an
17 extended period of time.

18 112. Further, identity thieves can combine data stolen in the data breach
19 with other information about Plaintiffs and Class members gathered from
20 underground sources, public sources, or even Plaintiffs' and Class members' social
21 media accounts. Thieves can use the combined data to send highly targeted
22 phishing emails to Plaintiffs and Class members to obtain more sensitive
23 information, placing Plaintiffs and Class members at further risk of harm. Thieves
24 can use the combined data to commit potential crimes, including opening new
25 financial accounts in Plaintiffs' and Class members' names, making false insurance
26 claims using Plaintiffs' and Class members' insurance information, taking out
27 loans in Plaintiffs' and Class members' names, using Plaintiffs' and Class
28 members' information to obtain government benefits, filing fraudulent tax returns

1 using Plaintiffs’ and Class members’ information, obtaining driver’s licenses in
2 Plaintiffs’ Class members’ names but with another person’s photograph.

3 113. Researchers at HealthITSecurity.com have also reported criminals
4 selling illicit access to compromised healthcare systems on the black market,
5 which would give other criminals “access to their own post-exploitation activity,
6 such as obtaining and exfiltrating sensitive information, infecting other devices in
7 the compromised network, or using connections and information in the
8 compromised network to exploit trusted relationships between the targeted
9 organizations and other entities to compromise additional networks.”

10 114. Given the value of e-PHI, health care providers such as Planned
11 Parenthood are prime targets for cyberattacks, like the data breach that occurred
12 here. Indeed, one recent report indicates that the number of healthcare cyberattacks
13 in the United States has increased by 55% between 2020 and 2021 alone.

14 115. Furthermore, with the news of the U.S. Supreme Court taking up the
15 politically charged Mississippi abortion law this court term and Texas’s recent
16 abortion law, abortion providers such as Planned Parenthood are likely targets for
17 cyberattacks like the data breach that occurred here given the nature of the
18 reproductive healthcare services they provide and the patients who utilize those
19 services.

20 116. More so than in a typical healthcare data breach, cybercriminals can
21 weaponize the highly sensitive and confidential e-PHI involved here to specifically
22 target and harass those patients, including Plaintiffs and Class members who
23 utilized Planned Parenthood’s reproductive healthcare services.

24 117. In 1997, an anti-abortion extremist named Neal Horsley created a
25 chilling website called the “Nuremberg Files.” The site contained the names of
26 about 200 working abortion providers with their approximate locations alongside
27 GIFs of dripping blood and encouragements to “SEND US MORE NAMES!” In
28 almost scorecard like fashion, if one of the providers was injured, his or her font

1 color turned from black to grey. If they were killed, their name was struck through.
2 David S. Cohen, Drexel University professor and co-author of the book *Living in*
3 *the Crosshairs: The Untold Stories of Anti-Abortion Terrorism*, has said that
4 publishing a list “is just another way for someone out there who wants to do harm
5 — and we know those people exist — to get more information that facilitates their
6 harm.”

7 118. Plaintiffs and Class members who utilized Planned Parenthood’s
8 services will now have to be on extremely high alert to protect their names and
9 addresses (which was one of the forms of e-PHI involved in the data breach) from
10 being made public to bad actors who may seek to threaten, harass, retaliate, or
11 intimidate them. No patient who utilizes Planned Parenthood should have to fear
12 for their lives or safety.

13 119. As to the imminent risk of fraud and identity theft, Plaintiffs and Class
14 members will be required to spend substantial amounts of time monitoring their
15 accounts for identity theft and fraud, the opening of fraudulent accounts, disputing
16 fraudulent transactions, and reviewing their financial affairs more closely than they
17 otherwise would have done but for the data breach. These efforts are burdensome
18 and time-consuming. Many Class members will also incur out-of-pocket costs for
19 protective measures such as identity theft protection, credit monitoring fees, credit
20 report fees, credit freeze fees, fees for replacement cards in the event of fraudulent
21 charges, and similar costs related to the data breach.

22 120. The risk of identity theft and fraud will persist for years. Identity
23 thieves often hold stolen data for months or years before using it to avoid
24 detection. Also, the sale of stolen information on the dark web may take months or
25 more to reach end-users, in part because the data is often sold in small batches as
26 opposed to in bulk to a single buyer. Thus, Plaintiffs and Class members must
27 vigilantly monitor their financial accounts indefinitely.
28

1 121. PPLA acknowledges that Plaintiffs and Class members face a
2 significant risk of various types of identity theft stemming from the data breach.
3 Attempting to shift the burden of responding to the data breach to patients, PPLA
4 recommended to Plaintiffs and affected patients that “[i]t is always a good idea to
5 review statements you receive from your health insurer and health care providers.
6 If you see charges for services you did not receive, please call the insurer or
7 provider immediately.” Thus, PPLA acknowledges that Plaintiffs and Class
8 members face an actual imminent risk of fraud and identity theft that requires not
9 only immediate action but continuous, ongoing monitoring.

10 122. Neither PPLA or PPFA has offered any credit or identity theft
11 monitoring to affected patients. Thus, what Planned Parenthood is doing is wholly
12 insufficient to combat the indefinite and undeniable risk of identity theft and fraud,
13 amongst other risks, that may continue long after the data breach.

14 123. Plaintiffs and Class members were also harmed because they were
15 promised services that Planned Parenthood represented would include reasonable
16 security measures to protect their highly sensitive and confidential e-PHI but that,
17 in reality, did not. Plaintiffs and Class members would not have used Planned
18 Parenthood’s services or provided their highly sensitive and confidential e-PHI had
19 they known that these representations were false.

20 124. Indeed, certain Plaintiffs specifically chose to seek sensitive medical
21 procedures at a Planned Parenthood facility because they did not feel comfortable
22 obtaining them from their primary doctor due to concerns for their privacy and
23 trusted that Planned Parenthood would maintain the privacy and confidentiality of
24 their highly sensitive and confidential e-PHI.

25 125. Lastly, Plaintiffs and Class members have been harmed by Planned
26 Parenthood’s intrusion upon their seclusion and invasion of their privacy rights, as
27 described in Section X. Planned Parenthood configured their systems in such a way
28 to make Plaintiffs’ and Class members’ highly sensitive and confidential e-PHI

1 exfiltrateable and available without their consent. As a result of Planned
2 Parenthood’s conduct, unauthorized persons did in fact access Plaintiffs’ and Class
3 members’ highly sensitive and confidential e-PHI, in which Plaintiffs and Class
4 members had a reasonable expectation of privacy.

5 **X. PLANNED PARENTHOOD’S PATIENTS HAVE A REASONABLE**
6 **EXPECTATION OF PRIVACY**

7 126. Plaintiffs and Class members have a reasonable expectation of privacy
8 in their intimate health data, which Planned Parenthood collected, stored, and
9 disclosed to unauthorized third parties.

10 127. It is woefully ironic that Planned Parenthood, an organizational
11 network of affiliates that prides itself on protecting and advocating for the right to
12 privacy and reproductive rights enshrined in the U.S. and California Constitutions
13 by affording patients reproductive healthcare access has allowed itself to be
14 susceptible to the data breach that exposed the highly sensitive and confidential e-
15 PHI of hundreds of thousands patients, including some of the most intimate details
16 of their private lives.

17 128. Plaintiffs and Class members have a reasonable expectation of privacy
18 in their highly sensitive and confidential e-PHI, which Planned Parenthood
19 collected, stored, and disclosed. This expectation of privacy is deeply enshrined in
20 California’s Constitution.

21 129. Article I, Section 1 of the California Constitution provides: “All
22 people are by nature free and independent and have inalienable rights. Among
23 these are enjoying and defending life and liberty, acquiring, possessing, and
24 protecting property, and pursuing and obtaining safety, happiness, *and privacy*.”
25 Art. I., Sec. 1, Cal. Const (emphasis added).

26 130. The phrase “and privacy” was added in 1972 after voters approved a
27 legislative constitutional amendment designated as Proposition 11. Critically, the
28 argument in favor of Proposition 11 reveals that the legislative intent was to curb

1 businesses’ control over the unauthorized collection and use of consumers’
2 personal information, stating in relevant part:

3 The right of privacy is the right to be left alone . . . It
4 prevents government and business interests from
5 collecting and stockpiling unnecessary information about
6 us and from misusing information gathered for one
7 purpose in order to serve other purposes or to embarrass
8 us.

8 **Fundamental to our privacy is the ability to control**
9 **circulation of personal information.** This is essential to
10 social relationships and personal freedom. The
11 proliferation of government and business records over
12 which we have no control limits our ability to control our
13 personal lives. Often we do not know that these records
14 even exist and we are certainly unable to determine who
15 has access to them.⁵

14 (emphasis added).

15 131. Consistent with this language, an abundance of studies examining the
16 collection of consumers’ personal data confirms that the surreptitious unauthorized
17 disclosure of highly sensitive and confidential e-PHI from hundreds of thousands
18 of individuals, as Planned Parenthood has done here, violates expectations of
19 privacy that have been established as general social norms.

20 132. Privacy polls and studies uniformly show that the overwhelming
21 majority of Americans consider one of the most important privacy rights to be the
22 need for an individual’s affirmative consent before a company collects and shares
23 its customers’ personal data.

24 133. Surveys consistently show that individuals care about the security and
25 privacy of their e-PHI. In 2013, the *Office of the National Coordinator for Health*

26 _____
27
28 ⁵ Ballot Pamp., Proposed Amends. to Cal. Const. with arguments to voters, Gen.
Elec. (Nov. 7, 1972) at 27.

1 *Information Technology* found that 7 out of 10 individuals are concerned about the
2 privacy of their medical records. The same study found that 3 out of 4 individuals
3 are concerned about the security of their medical records.

4 134. Likewise, a *Gallup* survey found that 78% of adults believe that it is
5 very important that their medical records be kept confidential, and a majority of
6 respondents believe no one should be permitted to see their records without consent.

7 135. A recent study by *Consumer Reports* shows that 92% of Americans
8 believe that internet companies and websites should be required to obtain consent
9 before sharing their data and the same percentage believe internet companies and
10 websites should be required to provide consumers with a complete list of the data
11 that has been collected about them.

12 136. Consistent with these expectations, Plaintiffs and Class members have
13 taken steps specifically to ensure the confidentiality of their medical information
14 and treatment at Planned Parenthood, including not disclosing this information to
15 others and even obscuring the specific treatment on insurance records.

16 137. Despite Plaintiffs and Class members expectation of privacy, Planned
17 Parenthood has failed to obtain adequate authorization and data security practices
18 in connection with its data collection practices and the unauthorized disclosure that
19 occurred. This constitutes a violation of Plaintiffs' and Class members' privacy
20 interests, including those explicitly enshrined in the California Constitution.

21 **CLASS ACTION ALLEGATIONS**

22 138. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P.
23 23(a), 23(b)(2) and (b)(3) on behalf of the following Nationwide Class:

24 All persons in the United States whose e-PHI was compromised in the
25 data breach that was made public by Planned Parenthood in November
26 2021. (the "**Nationwide Class**").

27 139. Excluded from the Nationwide Class are Defendants and its
28 subsidiaries and affiliates; all employees of Defendants and its subsidiaries and
affiliates; all persons who make a timely election to be excluded from the

1 Nationwide Class; Plaintiffs’ counsel and Planned Parenthood’s counsel and
2 members of their immediate families; government entities; and the judge to whom
3 this case is assigned, including his/her immediate family and court staff.

4 140. Plaintiffs reserve the right to modify, expand or amend the above
5 Class definitions or to seek certification of a class or classes defined differently
6 than above before any court determines whether certification is appropriate
7 following discovery.

8 **CALIFORNIA SUBCLASS**

9 141. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P.
10 23(a), 23(b)(2) and (b)(3) on behalf of the following California Subclass:

11 All persons in the state of California whose e-PHI were compromised
12 in the data breach that was made public by Planned Parenthood in
13 November 2021. (the “**California Subclass**”).

14 142. Excluded from the California Subclass are Defendants and its
15 subsidiaries and affiliates; all employees of Defendants and its subsidiaries and
16 affiliates; all persons who make a timely election to be excluded from the
17 California Class; Plaintiffs’ counsel and Planned Parenthood’s counsel and
18 members of their immediate families; government entities; and the judge to whom
19 this case is assigned, including his/her immediate family and court staff.

20 143. Plaintiffs reserve the right to modify, expand or amend the above
21 Subclass definitions or to seek certification of a class or classes defined
22 differently than above before any court determines whether certification is
23 appropriate following discovery.

24 **PAID NATIONWIDE SUBCLASS**

25 144. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P.
26 23(a), 23(b)(2) and (b)(3) on behalf of the following Paid Subclass:
27
28

1 All persons in the United States who paid money (including premiums)
2 to Planned Parenthood whose e-PHI was compromised in the data
3 breach that was made public by Planned Parenthood in November 2021.
(the “**Paid Nationwide Subclass**”).

4 145. Excluded from the Paid Subclass are Defendants and its subsidiaries
5 and affiliates; all employees of Defendants and its subsidiaries and affiliates; all
6 persons who make a timely election to be excluded from the California Class;
7 Plaintiffs’ counsel and Planned Parenthood’s counsel and members of their
8 immediate families; government entities; and the judge to whom this case is
9 assigned, including his/her immediate family and court staff.

10 146. Plaintiffs reserve the right to modify, expand or amend the above
11 Subclass definitions or to seek certification of a class or classes defined
12 differently than above before any court determines whether certification is
13 appropriate following discovery.

14 147. Certification of Plaintiffs’ claims for class-wide treatment are
15 appropriate because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are
16 satisfied. Plaintiffs can prove the elements of their claims on a class-wide basis
17 using the same evidence as would be used to prove those elements in individual
18 actions alleging the same claims.

19 **PAID CALIFORNIA SUBCLASS**

20 148. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P.
21 23(a), 23(b)(2) and (b)(3) on behalf of the following Paid Subclass:

22 All persons in California who paid money (including premiums) to
23 Planned Parenthood whose e-PHI was compromised in the data breach
24 that was made public by Planned Parenthood in November 2021. (the
“**Paid California Subclass**”).

25 149. Excluded from the Paid Subclass are Defendants and its subsidiaries
26 and affiliates; all employees of Defendants and its subsidiaries and affiliates; all
27 persons who make a timely election to be excluded from the California Class;
28 Plaintiffs’ counsel and Planned Parenthood’s counsel and members of their

1 immediate families; government entities; and the judge to whom this case is
2 assigned, including his/her immediate family and court staff.

3 150. Plaintiffs reserve the right to modify, expand or amend the above
4 Subclass definitions or to seek certification of a class or classes defined
5 differently than above before any court determines whether certification is
6 appropriate following discovery.

7 151. Certification of Plaintiffs' claims for class-wide treatment are
8 appropriate because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are
9 satisfied. Plaintiffs can prove the elements of their claims on a class-wide basis
10 using the same evidence as would be used to prove those elements in individual
11 actions alleging the same claims.

12 152. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are
13 satisfied. The members of the Classes are so numerous and geographically
14 dispersed that individual joinder of all Class members is impracticable. While
15 Plaintiffs are informed and believe that there are likely at least 400,000 members
16 of the Classes according to news reports, the precise number of Class members is
17 unknown to Plaintiffs. Class members may be identified through objective means
18 including Planned Parenthood's own patient records. Class members may be
19 notified of the pendency of this action by recognized, court-approved notice
20 dissemination methods, which may include U.S. mail, electronic mail, internet
21 postings, and/or published notice.

22 153. **Commonality and Predominance:** All requirements of Fed. R. Civ.
23 P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of
24 law and fact, which predominate over any questions affecting individual Class
25 members, including, without limitation:

26 a. Whether Defendants owed a duty to Plaintiffs and Class members to
27 secure and safeguard their e-PHI;

28

- 1 b. Whether Defendants failed to use reasonable care and reasonable
- 2 methods to secure and safeguard Plaintiffs’ and Class members’ e-
- 3 PHI;
- 4 c. Whether Defendants properly implemented security measures as
- 5 required by HIPAA or any other laws or industry standards to protect
- 6 Plaintiffs’ and Class members’ e-PHI from unauthorized access,
- 7 capture, dissemination and misuse;
- 8 d. Whether Plaintiffs and members of the Class were injured and
- 9 suffered damages and ascertainable losses as a result of Defendants’
- 10 actions or failure to act;
- 11 e. Whether Defendants engaged in active misfeasance and misconduct
- 12 alleged herein;
- 13 f. Whether Defendants knew or should have known that its data security
- 14 systems and monitoring processes were deficient;
- 15 g. Whether Defendants’ failure to provide adequate security proximately
- 16 caused Plaintiffs’ and Class members’ injuries; and
- 17 h. Whether Plaintiffs and Class members are entitled to declaratory and
- 18 injunctive relief.

19 154. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied.
20 Plaintiffs are members of the Classes. Plaintiffs’ claims are typical of the claims of
21 all Class members because Plaintiffs, like other Class members, suffered theft of
22 their e-PHI in the data breach.

23 155. **Adequacy of Representation:** All requirements of Fed. R. Civ. P.
24 23(a)(4) are satisfied. Plaintiffs are adequate Class representatives because they are
25 members of the Classes and their interests do not conflict with the interests of other
26 Class members that they seek to represent. Plaintiffs are committed to pursuing this
27 matter for the Classes with the Class’s collective best interest in mind. Plaintiffs
28 have retained counsel competent and experienced in complex class action litigation

1 of this type and Plaintiffs intend to prosecute this action vigorously. Plaintiffs, and
2 their counsel, will fairly and adequately protect the Class’s interests.

3 156. **Predominance and Superiority:** All requirements of Fed. R. Civ. P.
4 23(b)(3) are satisfied. As described above, common issues of law or fact
5 predominate over individual issues. Resolution of those common issues in
6 Plaintiffs’ case will also resolve them for the Class’s claims. In addition, a class
7 action is superior to any other available means for the fair and efficient
8 adjudication of this controversy and no unusual difficulties are likely to be
9 encountered in the management of this class action. The damages or other financial
10 detriment suffered by Plaintiffs and other Class members are relatively small
11 compared to the burden and expense that would be required to individually litigate
12 their claims against Planned Parenthood, so it would be impracticable for members
13 of the Class to individually seek redress for Planned Parenthood’s wrongful
14 conduct. Even if Class members could afford individual litigation, the court system
15 could not. Individualized litigation creates a potential for inconsistent or
16 contradictory judgments and increases the delay and expense to all parties and the
17 court system. By contrast, the class action device presents far fewer management
18 difficulties and provides the benefits of single adjudication, economies of scale,
19 and comprehensive supervision by a single court.

20 157. **Cohesiveness:** All requirements of Fed. R. Civ. P. 23(b)(2) are
21 satisfied. Planned Parenthood has acted, or refused to act, on grounds generally
22 applicable to the Class such that final declaratory or injunctive relief appropriate.

23 158. Plaintiffs reserve the right to revise the foregoing class allegations and
24 definitions based on facts learned and legal developments following additional
25 investigation, discovery, or otherwise.

1 **CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS**

2 159. California’s substantive laws apply to every member of the Class,
3 regardless of where in the United States the Class member resides.

4 160. California’s substantive laws may be constitutionally applied to the
5 claims of Plaintiffs and the Class under the Due Process Clause, 14th Amend. § 1,
6 and the Full Faith and Credit Clause, Art. IV § 1 of the U.S. Constitution.

7 California has significant contacts, or significant aggregation of contacts, to the
8 claims asserted by Plaintiffs and all Class members, thereby creating state interests
9 that ensure that the choice of California state law is not arbitrary or unfair.

10 161. PPLA is incorporated in California, its principal place of business is
11 located in California. PPLA also owns property and conducts substantial business
12 in California, and therefore California has an interest in regulating Planned
13 Parenthood’s conduct under its laws. PPLA’s decision to reside in California and
14 avail itself of California’s laws, and to engage in the challenged conduct from and
15 emanating out of California, renders the application of California law to the claims
16 herein constitutionally permissible.

17 162. California is also the state from which Planned Parenthood’s alleged
18 misconduct emanated. This conduct similarly injured and affected Plaintiffs and all
19 other Class members.

20 163. The application of California laws to the Class is also appropriate
21 under California’s choice of law rules because California has significant contacts
22 to the claims of Plaintiffs and the proposed Class and Subclasses, and California
23 has a greater interest in applying its laws here than any other interested state.

CLAIMS FOR RELIEF
COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class)

1
2
3
4 164. Plaintiffs re-allege and incorporate by reference all preceding
5 allegations as if fully set forth herein.

6 165. Planned Parenthood is a provider of reproductive healthcare services
7 whose patients, including Plaintiffs and Class members, entrust them with highly
8 sensitive and confidential e-PHI in connection with these services.

9 166. Given the highly sensitive nature of e-PHI and likelihood of harm
10 resulting from its unauthorized access, acquisition, use, or disclosure, multiple
11 statutes, regulations, and guidelines, in addition to the common law, impose a duty
12 on Planned Parenthood to protect this information.

13 167. For example, the HIPAA Security Rule requires Planned Parenthood
14 to: (a) ensure the confidentiality, integrity, and availability of all e-PHI they create,
15 receive, maintain or transmit; (b) proactively identify and protect against
16 reasonably anticipated threats to the security or integrity of the information; (c)
17 protect against reasonably anticipated, impermissible uses or disclosures; (d) put in
18 place the required administrative, physical and technical safeguards; (e) implement
19 policies and procedures to prevent, detect, contain, and correct security violations;
20 (f) effectively train their workforce regarding the proper handling of e-PHI; and (g)
21 designate individual security and privacy officers to ensure compliance.

22 168. Planned Parenthood also had a duty to use reasonable data security
23 measures under several state and federal laws, including § 5 of the FTC Act, which
24 prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted
25 and enforced by the FTC, the unfair practice of failing to use reasonable measures
26 to protect consumer data.
27
28

1 169. Planned Parenthood owed a duty of care to Plaintiffs and Class
2 members to provide data security consistent with the various statutory
3 requirements, regulations, and other notices described above.

4 170. Accordingly, Planned Parenthood owed a duty to Plaintiffs and Class
5 members to exercise reasonable care in safeguarding and protecting their highly
6 sensitive and confidential e-PHI by, among other things: (a) maintaining adequate
7 security systems to ensure that Plaintiffs’ and Class members’ highly sensitive and
8 confidential e-PHI was adequately secured and protected; (b) implementing
9 processes that would detect a breach of Planned Parenthood’s systems in a timely
10 manner; and (c) timely notifying patients, including Plaintiffs and Class members,
11 that their highly sensitive and confidential e-PHI had been accessed, acquired,
12 used, or disclosed as a result of a data breach so that Plaintiffs and Class members
13 could protect themselves from identify theft by transferring their records to a
14 different provider who maintained adequate security controls, obtaining credit
15 and/or identify theft monitoring protection, canceling or changing their bank
16 account and/or debit or credit card information, and/or taking other appropriate
17 precautions.

18 171. Planned Parenthood’s duty of care arose as a result of, among other
19 things, the special relationship that existed between Planned Parenthood and its
20 patients. Planned Parenthood was the only party in a position to ensure that its
21 systems were sufficient to protect against the foreseeable risk that a data breach
22 could occur, which would result in substantial harm to consumers.

23 172. Planned Parenthood was subject to an “independent duty” untethered
24 to any contract between Plaintiffs and Class members and Planned Parenthood.

25 173. Planned Parenthood breached their duty to exercise reasonable care in
26 safeguarding and protecting Plaintiffs’ and Class members’ highly sensitive and
27 confidential e-PHI by failing to adopt, implement, and maintain adequate security
28 measures.

1 174. For example, Planned Parenthood failed to implement appropriate
2 systems to detect a breach of their systems. Planned Parenthood negligently failed
3 to abide by the HIPAA Security Rule, among other guidelines and regulations, by
4 failing to protect against anticipated threats to the security or integrity of Plaintiffs’
5 and Class members’ highly sensitive and confidential e-PHI, and any reasonably
6 anticipated impermissible uses or disclosures of their highly sensitive and
7 confidential e-PHI.

8 175. Planned Parenthood also breached their duty to exercise reasonable
9 care in safeguarding and protecting Plaintiffs’ and Class members’ highly sensitive
10 and confidential e-PHI by failing to timely notify Plaintiffs and Class members that
11 their highly sensitive and confidential e-PHI had been accessed by unauthorized
12 third parties.

13 176. Planned Parenthood’s failure to comply with industry regulations such
14 as HIPAA further evidence their negligence in failing to exercise reasonable care
15 in safeguarding and protecting Plaintiffs’ and Class members’ highly sensitive and
16 confidential e-PHI.

17 177. It was foreseeable to Planned Parenthood that a failure to use
18 reasonable measures to protect its patients’ highly sensitive and confidential e-PHI
19 could result in injury to its patients.

20 178. Actual and attempted breaches of data security were reasonably
21 foreseeable to Planned Parenthood given that other PPFA affiliates had recently
22 been breached before as well as the known frequency of data breaches and various
23 warnings from industry experts.

24 179. The injuries and harm suffered by Plaintiffs and Class members as a
25 result of having their highly sensitive and confidential e-PHI accessed, viewed,
26 acquired, used, or disclosed without authorization was the reasonably foreseeable
27 result of Planned Parenthood’s failure to exercise reasonable care in safeguarding
28 and protecting Plaintiffs’ and Class members’ highly sensitive and confidential e-

1 PHI. Planned Parenthood knew or should have known that the systems and
2 technologies used for storing Plaintiffs’ and Class members’ highly sensitive and
3 confidential e-PHI allowed that information to be accessed, acquired, used, or
4 disclosed by unauthorized third parties. But for Planned Parenthood’s wrongful
5 and negligent breach of duties owed to Plaintiffs and Class members, the injuries
6 alleged herein would not have occurred.

7 180. In connection with the conduct described above, Planned Parenthood
8 acted wantonly, recklessly, and with complete disregard for the consequences
9 Plaintiffs and Class members would suffer if their highly sensitive and confidential
10 e-PHI was accessed by unauthorized third parties.

11 181. In addition to Planned Parenthood’s common law duty to exercise
12 reasonable care in securing Plaintiffs’ and Class members’ data, several statutes
13 independently imposed a duty on Planned Parenthood to safeguard highly sensitive
14 e-PHI. Planned Parenthood’s violation of these statutory duties, as described
15 below, each independently provides an evidentiary presumption to support
16 Plaintiffs’ and Class members’ negligence claim as negligence *per se*.

17 HIPAA

18 182. As alleged above, the HIPAA Security Rule requires Planned
19 Parenthood to maintain reasonable and appropriate administrative, technical, and
20 physical safeguards for protecting highly sensitive and confidential e-PHI, which
21 Planned Parenthood negligently failed to implement.

22 183. The HIPAA Security Rule also requires Planned Parenthood to protect
23 against reasonably anticipated threats to the security or integrity of e-PHI and
24 protect against reasonably anticipated impermissible uses or disclosures, which
25 Planned Parenthood negligently failed to do. *See* 45 C.F.R. Part 160 and Part 164,
26 Subpart A and C.

27
28

1 184. Planned Parenthood’s failure to secure Plaintiffs’ and Class members’
2 e-PHI and to notify them that such information had been accessed by unauthorized
3 third parties violated at least the following HIPAA regulations:

- 4 a. The HIPAA Privacy and Security Rule 45 C.F.R. § 160 and 45
5 C.F.R. § 164, Subpart A, C, and E
 - 6 i. 45 C.F.R. § 164.306
 - 7 ii. 45 C.F.R. § 164.308
 - 8 iii. 45 C.F.R. § 164.312
 - 9 iv. 45 C.F.R. § 164.314
 - 10 v. 45 C.F.R. § 164.502
 - 11 vi. 45 C.F.R. § 164.530

12 185. The harm that has occurred is the type of harm that HIPAA was
13 intended to guard against, namely, the disclosure of patients’ sensitive patient
14 information, including e-PHI.

15 186. Plaintiffs and Class members are within the class of persons that the
16 HIPAA Privacy and Security Rule were intended to protect, because the HIPAA
17 Privacy and Security rule were expressly designed to protect sensitive patient
18 information.

19 187. Planned Parenthood had a duty to Plaintiffs and Class members to
20 implement and maintain reasonable security procedures and practices under
21 HIPAA to safeguard Plaintiffs’ and Class members’ highly sensitive and
22 confidential e-PHI.

23 188. Planned Parenthood breached their duties to Plaintiffs and Class
24 members under the HIPAA, by failing to provide fair, reasonable, or adequate
25 computer systems and data security practices to safeguard Plaintiffs’ and Class
26 members’ highly sensitive and confidential e-PHI.

27 189. Planned Parenthood’s violations of HIPAA and its failure to comply
28 with applicable laws and regulations constitutes negligence *per se*.

1 FTC Act, 15 U.S.C. § 45

2 190. As alleged above, pursuant to the FTC Act, 15 U.S.C. § 45, Planned
3 Parenthood had a duty to provide fair and adequate computer systems and data
4 security practices to safeguard Plaintiffs’ and Class members’ highly sensitive and
5 confidential e-PHI.

6 191. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting
7 commerce,” including, as interpreted and enforced by the FTC, the failure to use
8 reasonable measures to protect highly sensitive and confidential e-PHI. The FTC
9 publications and orders described above also form part of the basis of Planned
10 Parenthood’s duty.

11 192. Planned Parenthood violated Section 5 of the FTC Act by failing to
12 use reasonable measures to protect highly sensitive and confidential e-PHI and
13 comply with applicable industry standards, including the FTC Act, as described in
14 detail herein. Planned Parenthood’s conduct was particularly unreasonable given
15 the nature and amount of e-PHI it collected and stored and the foreseeable
16 consequences of a data breach, including specifically, as described herein, the
17 damages that would result to consumers.

18 193. Plaintiffs and Class members are consumers within the class of
19 persons Section 5 of the FTC Act was intended to protect because they paid
20 Planned Parenthood for reproductive healthcare and/or medical goods and services.

21 194. The harm that has occurred is the type of harm the FTC Act was
22 intended to guard against, namely harm to consumers as a result of unfair practices
23 in commerce.

24 195. Indeed, the FTC has pursued numerous enforcement actions against
25 businesses that, as a result of their failure to employ reasonable data security
26 measures and avoid unfair and deceptive practices, caused the same harm as that
27 suffered by Plaintiffs and Class members.

1 196. Planned Parenthood had a duty to Plaintiffs and Class members to
2 implement and maintain reasonable security procedures and practices to safeguard
3 Plaintiffs’ and Class members’ highly sensitive and confidential e-PHI.

4 197. Planned Parenthood breached their duties to Plaintiffs and Class
5 members under the FTC Act, by failing to provide fair, reasonable, or adequate
6 computer systems and data security practices to safeguard Plaintiffs’ and Class
7 members’ highly sensitive and confidential e-PHI.

8 198. Planned Parenthood’s violations of Section 5 of the FTC Act and its
9 failure to comply with applicable laws and regulations constitutes negligence *per*
10 *se*.

11 California’s Confidentiality of Medical Information Act

12 Cal. Civ. Code § 56, et seq.

13 199. Under the CMIA, “[a]n electronic health record system or electronic
14 medical record system shall do the following: (A) Protect and preserve the
15 integrity of electronic medical information; [and] (B) Automatically record and
16 preserve any change or deletion of any electronically stored medical information.
17 The record of any change or deletion shall include the identity of the person who
18 accessed and changed the medical information, the date and time the medical
19 information was accessed, and the change that was made to the medical
20 information.” Cal. Civ. Code § 56.101(b)(1)(A) – (B).

21 200. Planned Parenthood violated the CMIA by negligently maintaining,
22 preserving, and storing Plaintiffs’ and Class members’ medical information
23 inasmuch as it did not implement adequate security protocols to prevent
24 unauthorized access to medical information, maintain an adequate electronic
25 security system to prevent data breaches, or employ industry standard and
26 commercially viable measures to mitigate the risks of any data the risks of any data
27 breach or otherwise comply with HIPAA data security requirements.
28

1 201. Planned Parenthood failed to protect and preserve the integrity of
2 electronic medical information and automatically record and preserve any change
3 or deletion of any electronically stored medical information.

4 202. Plaintiffs and Class members are within the class of persons the
5 CMIA is intended to protect against, namely, patients of health care providers.

6 203. The harm that has occurred is the type of harm the CMIA was
7 intended to guard against, namely protecting and preserving the integrity of
8 electronic medical information.

9 204. As a direct and proximate result of Planned Parenthood’s negligence,
10 Plaintiffs’ and Class members’ medical information was accessed and exfiltrated
11 by an unauthorized third party and they were injured as a result.

12 205. The injury and harm suffered by Plaintiffs and Class members was a
13 reasonably foreseeable result of Planned Parenthood’s breach of its duties. Planned
14 Parenthood knew or should have known that the breach of its duties would cause
15 Plaintiffs and Class members to suffer the foreseeable harms associated with the
16 exposure of their medical information.

17 206. Planned Parenthood’s violations of the CMIA constitutes negligence
18 *per se*.

19 207. As a direct and proximate result of Planned Parenthood’s negligence,
20 including violations of HIPAA, the FTC Act, and the CMIA constituting
21 negligence *per se*, Plaintiffs and Class members sustained damages, including
22 violation of their privacy interest and emotional distress, as alleged herein.
23 Plaintiffs and Class members are entitled to compensatory and consequential
24 damages suffered as a result of the data breach.

25 208. As a result of Defendants’ negligence, Plaintiffs and Class members
26 are also entitled to injunctive relief requiring Planned Parenthood to, among other
27 things: (i) strengthen its data security systems and monitoring procedures; (ii)
28

1 submit to future annual audits of those systems; and (iii) provide free credit
2 monitoring and identity theft insurance to Plaintiffs and all Class members.

3 **COUNT II**
4 **BREACH OF CONTRACT**
5 **(On behalf of the Nationwide Class)**

6 209. Plaintiffs re-allege and incorporate by reference all preceding
7 allegations as if fully set forth herein.

8 210. Planned Parenthood expressly promised to safeguard Plaintiffs' and
9 Class members' highly sensitive and confidential e-PHI in accordance with the
10 applicable state and federal laws and/or regulations. Additionally, Planned
11 Parenthood promised to abide by their own Privacy Policy, which they provided to
12 patients.

13 211. This Privacy Policy applied to Plaintiffs and Class members who
14 accepted Planned Parenthood's promise and entered into a contract with Planned
15 Parenthood when they entrusted their highly sensitive and confidential e-PHI to
16 Planned Parenthood as part of a transaction for medical goods and services.

17 212. Plaintiffs and Class members fully performed their obligations under
18 their contracts with Defendant, including by providing their highly sensitive and
19 confidential e-PHI and receiving treatment at Planned Parenthood.

20 213. Planned Parenthood did not hold up their end of the bargain. In
21 entering into such contracts, Planned Parenthood agreed to protect Plaintiffs' and
22 Class members' highly sensitive and confidential e-PHI, secure the servers and
23 systems that housed Plaintiffs' and Class members' highly sensitive and
24 confidential e-PHI, and to provide timely notice if their highly sensitive and
25 confidential e-PHI was accessed, acquired, used, or disclosed.

26 214. Planned Parenthood failed on all accounts: they failed to take
27 reasonable steps to protect Plaintiffs' and Class members' highly sensitive and
28 confidential e-PHI, secure their servers and systems that stored Plaintiffs' and
Class members' highly sensitive and confidential e-PHI. Each of these acts

1 constituted a separate breach of the contracts Planned Parenthood entered with
2 Plaintiffs and Class members.

3 215. Plaintiffs and Class members would not have entrusted Planned
4 Parenthood with their highly sensitive and confidential e-PHI in the absence of the
5 contract between them and Defendant, obligating Planned Parenthood to keep this
6 information secure and provide timely notice in the event of a breach.⁶

7 216. As a direct and proximate result of Planned Parenthood’s breaches of
8 their contracts, Plaintiffs and Class members sustained damages as alleged herein,
9 including when they received services that did not include reasonable security
10 measures sufficient to protect Plaintiffs’ and Class members’ highly sensitive and
11 confidential e-PHI, despite Planned Parenthood’s promise that it would do so.
12 Plaintiffs and Class members would not have paid for and used, or would have
13 paid less, for Planned Parenthood’s services had they known these representations
14 were false.

15 217. Plaintiffs and Class members are entitled to compensatory and
16 consequential damages as a result of Planned Parenthood’s breach of contract.

17 **COUNT III**
18 **BREACH OF IMPLIED CONTRACT**
19 **(On behalf of the Nationwide Class)**

20 218. Plaintiffs re-allege and incorporate by reference all preceding
21 allegations as if fully set forth herein.

22 219. When Plaintiffs and Class members provided their highly sensitive
23 and confidential e-PHI to Planned Parenthood in exchange for Planned
24 Parenthood’s services, they entered into implied contracts with Planned
25

26
27 ⁶ This is consistent with most consumer attitudes. A recent study by CynergisTek,
28 a leading cybersecurity firm, found that 70 percent of individuals would be likely
to cut ties with a healthcare provider who was not properly securing their personal
health data.

1 Parenthood under which Defendants agreed to take reasonable steps to protect their
2 highly sensitive and confidential e-PHI.

3 220. Planned Parenthood solicited and invited Plaintiffs and Class
4 members to provide their highly sensitive and confidential e-PHI as part of
5 Planned Parenthood’s regular business practices. Plaintiffs and Class members
6 accepted Planned Parenthood’s offers and provided their highly sensitive and
7 confidential e-PHI to Defendant.

8 221. When entering into the implied contracts, Plaintiffs and Class
9 members reasonably believed and expected that Planned Parenthood’s data
10 security practices complied with relevant laws, regulations, and industry standards.

11 222. When entering into the implied contracts, Plaintiffs and Class
12 members reasonably believed that Planned Parenthood would safeguard and
13 protect their highly sensitive and confidential e-PHI and that Planned Parenthood
14 would use part of the funds received from Plaintiffs and Class members to pay for
15 adequate and reasonable data security practices. Planned Parenthood failed to do
16 so.

17 223. Plaintiffs and Class members would not have provided their highly
18 sensitive and confidential e-PHI to Planned Parenthood in the absence of Planned
19 Parenthood’s implied promise to keep their highly sensitive and confidential e-PHI
20 reasonably secure.

21 224. Plaintiffs and Class members fully performed their obligations under
22 the implied contracts by paying money to Planned Parenthood.

23 225. Planned Parenthood breached its implied contracts with Plaintiffs and
24 Class members by failing to safeguard and protect their highly sensitive and
25 confidential e-PHI.

26 226. As a direct and proximate result of Planned Parenthood’s breaches of
27 implied contracts, Plaintiffs and Class members sustained damages as alleged
28 herein, including when they received services that did not include reasonable

1 security measures sufficient to protect Plaintiffs’ and Class members’ highly
2 sensitive and confidential e-PHI, despite Planned Parenthood’s promise that it
3 would do so. Plaintiffs and Class members would not have paid for and used, or
4 would have paid less, for Planned Parenthood’s services had they known these
5 representations were false.

6 227. Plaintiffs and Class members are also entitled to injunctive relief
7 requiring Planned Parenthood to, among other things: (i) strengthen its data
8 security systems and monitoring procedures; (ii) submit to future annual audits of
9 those systems; and (iii) provide free credit monitoring and identity theft insurance
10 to all Class members.

11 **COUNT IV**
12 **UNJUST ENRICHMENT**
13 **(On behalf of the Nationwide Class)**

14 228. Plaintiffs re-allege and incorporate by reference all preceding
15 allegations as if fully set forth herein.

16 229. Plaintiffs and Class members conferred a monetary benefit upon
17 Planned Parenthood when they paid money for services at Planned Parenthood.

18 230. Planned Parenthood appreciated or had knowledge of the benefits
19 conferred upon it by Plaintiffs and Class members. Planned Parenthood also
20 benefited from the receipt of Plaintiffs’ and Class members’ highly sensitive and
21 confidential e-PHI.

22 231. The funds Plaintiffs and Class members paid to Planned Parenthood
23 were supposed to be used by Planned Parenthood, in part, to pay for adequate data
24 privacy infrastructure, practices, and procedures.

25 232. As a result of Planned Parenthood’s conduct, Plaintiffs and Class
26 members suffered actual damages in an amount equal to the difference in value
27 between what they paid for, Planned Parenthood’s medical goods/services made
28 with adequate data privacy and security practices and procedures, and what they

1 received, Planned Parenthood’s medical goods/services without adequate data
2 privacy and security practices and procedures.

3 233. Under principals of equity and good conscience, Planned Parenthood
4 should not be permitted to retain the money belonging to Plaintiffs and Class
5 members because Planned Parenthood failed to implement, or adequately
6 implement, the data privacy and security practices and procedures that Plaintiffs
7 and Class members paid for and that were otherwise mandated by federal, state,
8 and local laws and industry standards.

9 234. Planned Parenthood should be compelled to disgorge into a common
10 fund for the benefit of Plaintiffs and Class members all unlawful or inequitable
11 proceeds received by it as a result of the conduct and data breach alleged herein.

12
13 **COUNT V**
14 **COMMON LAW INVASION OF PRIVACY – INTRUSION UPON**
15 **SECLUSION**
16 **(On behalf of the Nationwide Class)**

17 235. Plaintiffs re-allege and incorporate by reference all preceding
18 allegations as if fully set forth herein.

19 236. Plaintiffs asserting claims for intrusion upon seclusion must plead (1)
20 that the defendant intentionally intruded into a matter as to which plaintiff had a
21 reasonable expectation of privacy; and (2) that the intrusion was highly offensive
22 to a reasonable person.

23 237. There is no area where there is more of a reasonable expectation of
24 privacy than in the area of reproductive healthcare, which are the types of services
25 Planned Parenthood provides.

26 238. Planned Parenthood intentionally intruded upon the solitude, seclusion
27 and private affairs of Plaintiffs and Class members by intentionally configuring
28 their systems in such a way that left them vulnerable to malware/ransomware
attack, thus permitting unauthorized access to their systems, which compromised

1 Plaintiffs’ and Class members’ highly sensitive and confidential e-PHI. Only
2 Planned Parenthood had control over its systems.

3 239. Planned Parenthood’s conduct is especially egregious and offensive as
4 they failed to have any adequate security measures in place to prevent, track, or
5 detect in a timely fashion unauthorized access to Plaintiffs’ and Class members’ e-
6 PHI.

7 240. At all times, Planned Parenthood was aware that Plaintiffs’ and Class
8 members’ highly sensitive and confidential e-PHI in their possession contained
9 highly sensitive medical information, including patient name, and one or more of
10 the following: dates of birth, addresses, insurance identification numbers, and
11 clinical data (such as diagnosis, treatment, or prescription information).

12 241. Plaintiffs and Class members have a reasonable expectation in their e-
13 PHI, which contains highly sensitive medical information.

14 242. Planned Parenthood intentionally configured their systems in such a
15 way that stored Plaintiffs’ and Class Members’ highly sensitive and confidential e-
16 PHI to be left vulnerable to malware/ransomware attack without regard for
17 Plaintiffs’ and Class members’ privacy interests.

18 243. The disclosure of the highly sensitive and confidential e-PHI of
19 400,000 patients, was highly offensive to Plaintiffs and Class members because it
20 violated expectations of privacy that have been established by general social
21 norms, including by granting access to information and data that is private and
22 would not otherwise be disclosed.

23 244. Surveys consistently show that individuals care about the security and
24 privacy of their highly sensitive and confidential e-PHI. In 2013, the *Office of the*
25 *National Coordinator for Health Information Technology* found that 7 out of 10
26 individuals are concerned about the privacy of their medical records. The same
27 study found that 3 out of 4 individuals are concerned about the security of their
28 medical records. Likewise, a *Gallup* survey found that 78% of adults believe that it

1 is very important that their medical records be kept confidential, and a majority of
2 respondents believe no one should be permitted to see their records without
3 consent. Plaintiffs and Class members acted consistent with these polls and surveys
4 by safeguarding their medical information, including the ePHI exfiltrated and
5 stolen in the data breach.

6 245. Planned Parenthood’s conduct would be highly offensive to a
7 reasonable person in that it violated statutory and regulatory protections designed
8 to protect highly sensitive medical information, in addition to social norms.
9 Planned Parenthood’s conduct would be especially egregious to a reasonable
10 person as Planned Parenthood publicly disclosed Plaintiffs’ and Class members’
11 highly sensitive and confidential e-PHI without their consent, including to an
12 “unauthorized person,” i.e., hackers.

13 246. As a result of Planned Parenthood’s actions, Plaintiffs and Class
14 members have suffered harm and injury, including but not limited to an invasion of
15 their privacy rights.

16 247. Plaintiffs and Class members have been damaged as a direct and
17 proximate result of Planned Parenthood’s intrusion upon seclusion and are entitled
18 to just compensation.

19 248. Plaintiffs and Class members are entitled to appropriate relief,
20 including compensatory damages for the harm to their privacy, loss of valuable
21 rights and protections, and heightened risk of future invasions of privacy.

22 **COUNT VI**
23 **INVASION OF PRIVACY**
24 **ART. I, SEC 1 OF THE CALIFORNIA CONSTITUTION**
25 **(On behalf of the California Subclass)**

26 249. Plaintiffs re-allege and incorporate by reference all preceding
27 allegations as if fully set forth herein.

28 250. Art. I, § 1 of the California Constitution provides: “All people are by
nature free and independent and have inalienable rights. Among these are enjoying

1 and defending life and liberty, acquiring, possessing, and protecting property, and
2 pursuing and obtaining safety, happiness, and privacy.” Art. I, § 1, Cal. Const.

3 251. The right to privacy in California’s constitution creates a private right
4 of action against private and government entities.

5 252. To state a claim for invasion of privacy under the California
6 Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2)
7 a reasonable expectation of privacy; and (3) an intrusion so serious in nature,
8 scope, and actual or potential impact as to constitute an egregious breach of the
9 social norms.

10 253. Planned Parenthood violated Plaintiffs’ and California Subclass
11 members’ constitutional right to privacy by collecting, storing, and disclosing (1)
12 e-PHI in which they had a legally protected privacy interest, (2) Plaintiffs’ and
13 California Subclass members’ e-PHI in which they had a reasonable expectation
14 of privacy in, (3) in a manner that was highly offensive to Plaintiffs and California
15 Subclass members, would be highly offensive to a reasonable person, and was in
16 egregious violation of social norms.

17 254. Planned Parenthood have intruded upon Plaintiffs’ and California
18 Subclass members’ legally protected privacy interests, including, *inter alia*: (i)
19 interests in precluding the dissemination or misuse of sensitive and confidential
20 personal—the e-PHI; and (ii) interests in making intimate personal healthcare
21 decisions or conducting personal activities without observation, intrusion, or
22 interference.

23 255. The highly sensitive and confidential e-PHI, which Planned
24 Parenthood stored, monitored, collected, and disclosed without Plaintiffs’ and
25 California Subclass members’ authorization and/or consent included, *inter alia*,
26 patient names, dates of birth, addresses, insurance identification numbers, and
27 clinical data (such as diagnosis, treatment, or prescription information).
28

1 256. Plaintiffs and California Subclass members had a legally protected
2 informational privacy interest in the confidential and sensitive e-PHI involved as
3 well as a privacy interest in conducting their personal healthcare decisions and
4 activities without intrusion, interference, or disclosure.

5 257. Planned Parenthood’s actions constituted a serious invasion of privacy
6 that would be highly offensive to a reasonable person in that: (i) the invasion
7 occurred within a zone of privacy protected by the California Constitution, namely
8 the misuse of information gathered for an improper purpose; and (ii) the invasion
9 deprived Plaintiffs and California Subclass members of the ability to control the
10 circulation of their highly sensitive and confidential e-PHI, which is considered
11 fundamental to the right to privacy.

12 258. Plaintiffs and California Subclass members had a reasonable
13 expectation of privacy in that: (i) Planned Parenthood’s invasion of privacy
14 occurred as a result of Planned Parenthood’s security practices including the
15 collecting, storage, and unauthorized disclosure of highly sensitive and confidential
16 e-PHI; (ii) Plaintiffs and California Subclass members did not consent or otherwise
17 authorize Planned Parenthood to disclosure their highly sensitive and confidential
18 e-PHI; and (iii) Plaintiffs and California Subclass members could not reasonably
19 expect Planned Parenthood would commit acts in violation of laws protecting
20 privacy.

21 259. As a result of Planned Parenthood’s actions, Plaintiffs and California
22 Subclass members have been damaged as a direct and proximate result of Planned
23 Parenthood’s invasion of their privacy and are entitled to just compensation.

24 260. Plaintiffs and California Subclass members suffered actual and
25 concrete injury as a result of Planned Parenthood’s violations of their privacy
26 interests. Plaintiffs and California Subclass members are entitled to appropriate
27 relief, including damages to compensate them for the harm to their privacy
28 interests, loss of valuable rights and protections, heightened risk of future invasions

1 of privacy, and the mental and emotional distress and harm to human dignity
2 interests caused by Defendants’ invasions.

3 261. Plaintiffs and the California Subclass seek appropriate relief for that
4 injury, including but not limited to damages that will reasonably compensate
5 Plaintiffs and California Subclass members for the harm to their privacy interests
6 as well as disgorgement of profits made by Planned Parenthood as a result of its
7 intrusions upon Plaintiffs’ and California Subclass members’ privacy.

8
9 **COUNT VII**
10 **VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW**
11 **Cal. Bus. & Prof. Code § 17200, *et seq.***
12 **(On Behalf of the California Subclass)**

13 262. Plaintiffs re-allege and incorporate by reference all preceding
14 allegations as if fully set forth herein.

15 263. Planned Parenthood is a “person” as defined by Cal. Bus. & Prof.
16 Code §17201.

17 264. Planned Parenthood violated Cal. Bus. & Prof. Code §§ 17200, *et*
18 *seq.* (“UCL”) by engaging in unlawful, unfair, and deceptive business acts and
19 practices.

20 265. Planned Parenthood’s business acts and practices are “unlawful”
21 under the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et. seq.*
22 (“UCL”), because, as alleged above, Planned Parenthood violated the California
23 common law, California Constitution, and the other state and federal statutes and
24 causes of action described herein.

25 266. Planned Parenthood’s business acts and practices are “unfair” under
26 the UCL, because, as alleged above, California has a strong public policy of
27 protecting consumers’ privacy interests, including protecting consumers’ personal
28 data, including highly sensitive and confidential e-PHI. Planned Parenthood
violated this public policy by, among other things, surreptitiously collecting,

1 storing, disclosing, and otherwise misusing Plaintiffs’ and California Subclass
2 members’ highly sensitive and confidential e-PHI without Plaintiffs’ and
3 California Subclass members’ consent. Planned Parenthood further engaged in
4 unfair business practices because it made material misrepresentations and
5 omissions concerning the information that Planned Parenthood assured patients it
6 would protect their highly sensitive and confidential e-PHI, which deceived and
7 misled patients. Planned Parenthood’s conduct violates the policies of the statutes
8 referenced herein.

9 267. Planned Parenthood’s business acts and practices are also “unfair” in
10 that they are immoral, unethical, oppressive, unscrupulous, and/or substantially
11 injurious to consumers. The gravity of the harm of Planned Parenthood’s
12 collecting, storing, disclosing, and otherwise misusing Plaintiffs’ and California
13 Subclass members’ highly sensitive and confidential e-PHI is significant, and there
14 is no corresponding benefit resulting from such conduct. Finally, because Plaintiffs
15 and California Subclass members were completely unaware of Planned
16 Parenthood’s conduct, they could not have possibly avoided the harm.

17 268. Planned Parenthood’s business acts and practices are also “fraudulent”
18 within the meaning of the UCL. Planned Parenthood misrepresented that it
19 maintained sufficient data security measures and systems to protect Plaintiffs’ and
20 California Subclass members’ e-PHI. Planned Parenthood never disclosed that
21 these practices were severely deficient.

22 269. Planned Parenthood’s unlawful, unfair, and deceptive acts and
23 practices include:

- 24 (a) Failing to implement and maintain reasonable security and privacy
25 measures to protect Plaintiffs’ and California Subclass members’ e-
26 PHI, which was a direct and proximate cause of the data breach and
27 omitting, suppressing, and concealing the material fact of that
28 failure;

- 1 (b) Failing to identify foreseeable security and privacy risks, remediate
2 identified security and privacy risks, and adequately improve
3 security and privacy measures following well-publicized
4 cybersecurity incidents, which was a direct and proximate cause of
5 the data breach and omitting, suppressing, and concealing the
6 material fact of that failure;
- 7 (c) Failing to comply with common law and statutory duties pertaining
8 to the security and privacy of Plaintiffs' and California Subclass
9 members' e-PHI, including duties imposed by the FTC Act, HIPAA,
10 and CMIA which was a direct and proximate cause of the data
11 breach and omitting, suppressing, and concealing the material fact of
12 that failure;
- 13 (d) Misrepresenting that it would protect the privacy and confidentiality
14 of Plaintiffs' and California Subclass members' e-PHI, including by
15 implementing and maintaining reasonable security measures;
- 16 (e) Misrepresenting that it would comply with common law and
17 statutory duties pertaining to the security and privacy of Plaintiffs'
18 and California Subclass members' e-PHI, including duties imposed
19 by the FTC Act, HIPAA, and CMIA;
- 20 (f) Omitting, suppressing, and concealing the material fact that it did not
21 reasonably or adequately secure Plaintiffs' and California Subclass
22 members' e-PHI; and
- 23 (g) Omitting, suppressing, and concealing the material fact that it did not
24 comply with common law and statutory duties pertaining to the
25 security and privacy of Plaintiffs' and California Subclass members'
26 e-PHI, including duties imposed by the FTC Act, HIPAA, and the
27 CMIA.
28

1 270. Planned Parenthood’s representations and omissions were material
2 because they were likely to deceive reasonable consumers about the adequacy of
3 Planned Parenthood’s data security and ability to protect the confidentiality of
4 consumers’ highly sensitive and confidential e-PHI.

5 271. As a direct and proximate result of Planned Parenthood’s unfair,
6 unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass
7 members were injured and lost money or property, i.e., the prices received by
8 Planned Parenthood for its goods and medical services; the loss of the benefit of
9 their bargain with Planned Parenthood as they would not have paid Planned
10 Parenthood for goods and services or would have paid less for such goods and
11 services but for Planned Parenthood’s violations alleged herein; costs to be spent
12 for credit monitoring and identity protection services; time and expenses related
13 to monitoring their financial accounts for fraudulent activity; loss of value of
14 their highly sensitive and confidential e-PHI; and an increased, imminent risk of
15 fraud and identity theft.

16 272. Planned Parenthood’s violations were, and are, willful, deceptive,
17 unfair, and unconscionable.

18 273. Plaintiffs and California Subclass members would not have paid for
19 Planned Parenthood’s services, or would have paid significantly less, had they
20 known that its representations and omissions concerning data security were false.

21 274. Plaintiffs and California Subclass members have lost money and
22 property as a result of Planned Parenthood’s conduct in violation of the UCL, as
23 stated in herein and above. Health data, such as the e-PHI collected by Planned
24 Parenthood, objectively has value. For instance, Pfizer annually pays
25 approximately \$12 million to purchase health data from various sources.

26 275. Consumers and patients, including Plaintiffs and California Subclass
27 members also value their health data. According to the annual Financial Trust
28 Index Survey, conducted by *the University of Chicago’s Booth School of Business*

1 and Northwestern University’s Kellogg School of Management, which interviewed
2 more than 1,000 Americans, 93% would not share their health data with a digital
3 platform for free. Half of the survey respondents would only share their data for
4 \$100,000 or more, and 22% would only share their data if they received between
5 \$1,000 and \$100,000.

6 276. By deceptively storing, collecting, and disclosing this highly sensitive
7 and confidential e-PHI, Planned Parenthood has taken money or property from
8 Plaintiffs and California Subclass members.

9 277. Plaintiffs and California Subclass members seek all monetary and
10 non-monetary relief allowed by law, including compensatory damages;
11 restitution; disgorgement; punitive damages; injunctive relief; and reasonable
12 attorneys’ fees and costs.

13 **COUNT VIII**
14 **VIOLATION OF THE CALIFORNIA**
15 **CONSUMER LEGAL REMEDIES ACT**
16 **Cal. Civ. Code § 1750, et seq.**

17 **(On behalf of the Paid Nationwide Subclass and Paid California Subclass)**

18 278. Plaintiffs Pawlukiewicz and Dilanchyan re-allege and incorporate by
19 reference all preceding allegations as if fully set forth herein.

20 279. The Consumers Legal Remedies Act, Cal. Civ. Code § 1750, et seq.
21 (“CLRA”) is a comprehensive statutory scheme to protect consumers against
22 unfair and deceptive business practices in connection with the conduct of
23 businesses providing goods, property or services to consumers primarily for
24 personal, family, or household use.

25 280. Planned Parenthood is a “person” as defined by Civil Code §§
26 1761(c) and 1770 and has provided “services” as defined by Civil Code §§
27 1761(b) and 1770.

28 281. Civil Code section 1770, subdivision (a)(5) prohibits one who is
involved in a transaction from “[r]epresenting that goods or services have

1 sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities
2 which they do not have.”

3 282. Civil Code section 1770, subdivision (a)(7) prohibits one who is
4 involved in a transaction from “[r]epresenting that goods or services are of a
5 particular standard, quality, or grade . . . if they are of another.”

6 283. Plaintiffs Pawlukiewicz and Dilanchyan and members of the Paid
7 Subclass are “consumers” as defined by Civil Code §§ 1761(d) and 1770 and
8 have engaged in a “transaction” as defined by Civil Code §§ 1761(e) and 1770.

9 284. Planned Parenthood’s acts and practices were intended to and did
10 result in the sale of products and services to Plaintiffs and Paid Subclass members
11 in violation of Civil Code § 1770, including, but not limited to, the following:

- 12 (a) Representing that goods or services have characteristics that they do
13 not have;
- 14 (b) Representing that goods or services are of a particular standard,
15 quality, or grade when they were not;
- 16 (c) Advertising goods or services with intent not to sell them as
17 advertised;
- 18 (d) Representing that the subject of a transaction has been supplied in
19 accordance with a previous representation when it has not; and
- 20 (e) Representing the transaction confers or involves rights, remedies, or
21 obligations that it does not have or that are prohibited by law.

22 285. Planned Parenthood’s representations and omissions were material
23 because they were likely to and did deceive reasonable consumers about the
24 adequacy of Planned Parenthood’s data security and ability to protect the
25 confidentiality of patients’ highly sensitive and confidential e-PHI.

26 286. Had Planned Parenthood disclosed to Plaintiffs Pawlukiewicz and
27 Dilanchyan and Paid Nationwide Subclass members and Paid California Subclass
28 members that its data systems were not secure and, thus, vulnerable to attack,

1 Planned Parenthood would have been unable to continue in business and it would
2 have been forced to adopt reasonable data security measures and comply with the
3 law. Instead, Planned Parenthood received, maintained, and compiled Plaintiffs'
4 and Paid Subclass members' highly sensitive and confidential e-PHI as part of the
5 services Planned Parenthood provided and for which Plaintiffs Pawlukiewicz and
6 Dilanchyan and Paid Subclass members paid without advising them that Planned
7 Parenthood's data security practices were insufficient to maintain the safety and
8 confidentiality of their highly sensitive and confidential e-PHI. Accordingly,
9 Plaintiffs Pawlukiewicz and Dilanchyan and Paid Subclass members acted
10 reasonably in relying on Planned Parenthood's misrepresentations and omissions,
11 the truth of which they could not have discovered.

12 287. As a direct and proximate result of Planned Parenthood's violations
13 of California Civil Code § 1770, Plaintiffs Pawlukiewicz and Dilanchyan and Paid
14 Nationwide Subclass members and Paid California Subclass members have
15 suffered and will continue to suffer injury, ascertainable losses of money or
16 property, and monetary and non-monetary damages, including loss of the benefit
17 of their bargain with Planned Parenthood as they would not have paid Planned
18 Parenthood for goods and services or would have paid less for such goods and
19 services but for Planned Parenthood's violations alleged herein; costs for credit
20 monitoring and identity protection services; time and expenses related to
21 monitoring their financial accounts for fraudulent activity; loss of value of their
22 highly sensitive and confidential e-PHI; and an increased, imminent risk of fraud
23 and identity theft.

24 288. Plaintiffs Pawlukiewicz and Dilanchyan, individually and on behalf
25 of the Paid Nationwide Subclass members and Paid California Subclass members,
26 seeks an injunction requiring Planned Parenthood to adopt reasonable and
27 sufficient data security measures designed to protect and secure their highly
28 sensitive and confidential e-PHI.

1 individually identifiable information in the possession or derived from Planned
2 Parenthood.

3 293. Under the CMIA, “provider of health care” means “any person
4 licensed or certified pursuant to Division 2 (commencing with Section 500) of the
5 Business and Professions Code; any person licensed pursuant to the Osteopathic
6 Initiative Act or the Chiropractic Initiative Act; any person certified pursuant to
7 Division 2.5 (commencing with Section 1797) of the Health and Safety Code; any
8 clinic, health dispensary, or health facility licensed pursuant to Division 2
9 (commencing with Section 1200) of the Health and Safety Code.” Cal. Civ. Code §
10 56.05(m).

11 294. Planned Parenthood as a “provider of health care” is subject to the
12 CMIA, because it is a “business organized for the purpose of maintaining medical
13 information, as defined in subdivision (j) of Section 56.05, in order to make the
14 information available to an individual or to a provider of health care at the request
15 of the individual or a provider of health care, for purposes of allowing the
16 individual to manage his or her information, or for the diagnosis and treatment of
17 the individual, shall be deemed to be a provider of health care subject to the
18 requirements of this part.” Cal. Civ. Code § 56.06(a). As such, Planned
19 Parenthood is subject to the penalties for improper use and disclosure of medical
20 information prescribed in this part.” Cal. Civ. Code § 56.06(e).

21 295. Under the CMIA, “patient” means “any natural person, whether or not
22 still living, who received health care services from a provider of health care and to
23 whom medical information pertains. Cal. Civ. Code § 56.05(k).” Plaintiffs and
24 California Subclass members are “patients” under the CMIA.

25 296. Under the CMIA, “authorized recipient” means “any person who is
26 authorized to receive medical information pursuant to Section 56.10 or 56.20. Cal.
27 Civ. Code § 56.05(b).” Planned Parenthood is a “authorized recipient” under the
28 CMIA.

1 297. Planned Parenthood stored in electronic form on its computer system
2 Plaintiffs’ and California Subclass members’ “medical information” as defined by
3 Cal. Civ. Code § 56.05(j).

4 298. Planned Parenthood’s systems were designed, in part, to make
5 medical information available to Planned Parenthood so it could store, access, and
6 manage patients’ medical information, including but not limited to diagnosing,
7 treating, or managing patients’ medical conditions.

8 299. Under the CMIA, “[a] provider of health care, health care service
9 plan, or contractor shall not disclose medical information regarding a patient of the
10 provider of health care or an enrollee or subscriber of a health care service plan
11 without first obtaining an authorization, except as provided in subdivision (b) or
12 (c).” Cal. Civ. Code § 56.10(a).

13 300. Planned Parenthood violated Cal. Civ. Code § 56.10(a) as Plaintiffs
14 and California Subclass members did not provide Planned Parenthood
15 authorization nor was Planned Parenthood otherwise authorized to disclose
16 Plaintiffs’ or California Subclass members’ medical information to an
17 unauthorized third-party.

18 301. As a direct and proximate result of Planned Parenthood’s violation of
19 Cal. Civ. Code Section 56.10(a), Plaintiffs’ and California Subclass members’
20 medical information was viewed by an unauthorized third party.

21 302. Planned Parenthood’s unauthorized disclosures of Plaintiffs’ and
22 California Subclass members’ medical information has caused injury to Plaintiffs
23 and California Subclass members.

24 303. In addition, Cal. Civil Code Section 56.101, subdivision (a), requires
25 that every provider of health care “who creates, maintains, preserves, stores,
26 abandons, destroys, or disposes of medical information shall do so in a manner that
27 preserves the confidentiality of the information contained therein.”
28

1 304. Further, “[a]n electronic health record system or electronic medical
2 record system shall do the following:(A) Protect and preserve the integrity of
3 electronic medical information; [and] (B) Automatically record and preserve any
4 change or deletion of any electronically stored medical information. The record of
5 any change or deletion shall include the identity of the person who accessed and
6 changed the medical information, the date and time the medical information was
7 accessed, and the change that was made to the medical information.” Cal. Civ.
8 Code § 56.101(b)(1)(A) – (B).

9 305. Planned Parenthood failed to maintain, preserve, and store medical
10 information in a manner that preserves the confidentiality of the information
11 contained therein because it disclosed to third parties Plaintiffs’ and California
12 Subclass members’ highly sensitive and confidential e-PHI without consent.

13 306. As described throughout this Complaint, Planned Parenthood also
14 violated Cal. Civ. Code § 56.101(a) by negligently maintaining, preserving, and
15 storing Plaintiffs’ and California Subclass members’ medical information
16 inasmuch as it did not implement adequate security protocols to prevent
17 unauthorized access to medical information, maintain an adequate electronic
18 security system to prevent data breaches, or employ industry standard and
19 commercially viable measures to mitigate the risks of any data the risks of any data
20 breach or otherwise comply with HIPAA data security requirements.

21 307. Planned Parenthood failed to protect and preserve the integrity of
22 electronic medical information and automatically record and preserve any change
23 or deletion of any electronically stored medical information.

24 308. As a direct and proximate result of Planned Parenthood’s violation of
25 Cal. Civ. Code Section 56.101(a), Plaintiffs’ and California Subclass members’
26 medical information was viewed by an unauthorized third party.

1 309. Planned Parenthood’s negligent maintenance, preservation, and
2 storage of Plaintiffs’ and California Subclass members’ medical information has
3 caused injury to Plaintiffs and California Subclass members.

4 310. Accordingly, Plaintiffs and California Subclass members are entitled
5 to: (1) nominal damages of \$1,000 per violation; (2) actual damages, in an amount
6 to be determined at trial; (3) statutory damages pursuant to 56.36(c); (4) punitive
7 damages pursuant to Cal. Civ. Code Section 56.35; and (5) reasonable attorneys’
8 fees and other litigation costs reasonably incurred.

9 **COUNT X**
10 **REQUEST FOR RELIEF UNDER THE DECLARATORY JUDGMENT**
11 **ACT**

12 **28 U.S.C. § 2201, et seq.**
13 **(On Behalf of the Nationwide Class)**

14 311. Plaintiffs re-allege and incorporate by reference all preceding
15 allegations as if fully set forth herein.

16 312. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this
17 Court is authorized to enter a judgment declaring the rights and legal relations of
18 the parties and grant further necessary relief. Furthermore, the Court has broad
19 authority to restrain acts, such as here, that are tortious and violate the terms of the
20 statutes described in this Complaint.

21 313. An actual controversy has arisen in the wake of the data breach
22 regarding Planned Parenthood’s present and prospective common law and statutory
23 duties to reasonably safeguard its patients’ highly sensitive and confidential e-PHI
24 and whether Planned Parenthood is currently maintaining data security measures
25 adequate to protect Plaintiffs and Class members from further data breaches.
26 Plaintiffs allege that Planned Parenthood’s data security practices remain
27 inadequate.

28 314. Plaintiffs and Class members continue to suffer injury as a result of
the compromise of their highly sensitive and confidential e-PHI and remain at

1 imminent risk that further compromises of their personal information will occur in
2 the future.

3 315. Pursuant to its authority under the Declaratory Judgment Act, this
4 Court should enter a judgment declaring that Planned Parenthood continues to owe
5 a legal duty to secure consumers' highly sensitive and confidential e-PHI, to timely
6 notify consumers of any data breach, and to establish and implement data security
7 measures that are adequate to secure its patients' highly sensitive and confidential
8 e-PHI.

9 316. The Court also should issue corresponding prospective injunctive
10 relief requiring Planned Parenthood to employ adequate security protocols
11 consistent with law and industry standards to protect patients' highly sensitive and
12 confidential e-PHI.

13 317. If an injunction is not issued, Plaintiffs and Class members will suffer
14 irreparable injury, for which they lack an adequate legal remedy. The threat of
15 another data breach is real, immediate, and substantial. If another breach at
16 Planned Parenthood occurs, Plaintiffs and Class members will not have an
17 adequate remedy at law, because many of the resulting injuries are not readily
18 quantified and they will be forced to bring multiple lawsuits to rectify the same
19 conduct.

20 318. The hardship to Plaintiffs and Class members if an injunction does not
21 issue greatly exceeds the hardship to Planned Parenthood if an injunction is issued.
22 If another data breach occurs at Planned Parenthood, Plaintiffs and Class members
23 will likely be subjected to substantial identify theft and other damages. On the
24 other hand, the cost to Planned Parenthood of complying with an injunction by
25 employing reasonable prospective data security measures is relatively minimal,
26 and Planned Parenthood has a pre-existing legal obligation to employ such
27 measures.

28

1 319. Issuance of the requested injunction will serve the public interest by
2 preventing another data breach at Planned Parenthood, thus eliminating the
3 additional injuries that would result to Plaintiffs and the millions of consumers
4 whose confidential information would be further compromised.

5 **COUNT XI**
6 **VIOLATION OF THE CALIFORNIA CONSUMER RECORDS ACT**
7 **Cal. Civ. Code § 1798.80 *et seq.***
8 **(On Behalf of the California Subclass)**

9 320. Plaintiffs re-allege and incorporate by reference all preceding
10 allegations as if fully set forth herein.

11 321. Section 1798.2 of the California Civil Code requires any “person or
12 business that conducts business in California, and that owns or licenses
13 computerized data that includes personal information” to “disclose any breach of
14 the security of the system following discovery or notification of the breach in the
15 security of the data to any resident of California [] whose unencrypted personal
16 information was, or is reasonably believed to have been, acquired by an
17 unauthorized person...” Under section 1798.82, the disclosure “shall be made in
18 the most expedient time possible and without unreasonably delay...”

19 322. The California Consumer Records Act (“CCRA”) further provides:
20 “Any person or business that maintains computerized data that includes personal
21 information that the person or business does not own shall notify the owner or
22 licensee of the information of any breach of the security of the data immediately
23 following discovery, if the personal information was, or is reasonably believed to
24 have been, acquired by an unauthorized person.” Cal. Civ. Code § 1798.82(b).

25 323. Plaintiff and the California Subclass members are residents of
26 California and are “consumers” within the meaning of California Civil Code §
27 1798.80(c).

28 324. Defendants are “business(es)” within the meaning of California Civil
Code § 1798.80(a) which includes “a sole proprietorship, partnership, corporation,

1 association, or other group, however organized and whether or not organized to
2 operate at a profit.”

3 325. The data breach was a breach of security within the meaning of
4 section 1798.82. The PHI and e-PHI stolen constitutes “personal information”
5 within the meaning of California Civil Code §1798.80.

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

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

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

12 i. The name and contact information of the reporting person
13 or business subject.

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

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

18 1. The date of the breach;

19 2. The estimated date of the breach; or

20 3. The date range within which the breach occurred.

21 The notification shall also include the date of the
22 notice.

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

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

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

5 327. In violation of the CCRA, Defendants unreasonably delayed in
6 notifying Plaintiffs and members of the California Subclass of the data breach, in
7 which they were aware on or before October 17, 2021.

8 328. As a result of Defendants’ violation of Cal. Civ. Code § 1798.82(b),
9 Plaintiff and California Subclass members were deprived of prompt notice of the
10 data breach and were thus prevented from taking appropriate protective measures,
11 such as securing identity theft protection, as well as future costs related to the
12 same. These measures could have prevented some of the damages Plaintiff and
13 California Subclass members have suffered and will suffer because their PHI and
14 e-PHI would have had less value to identity thieves.

15 329. As a result of Defendants’ violation Cal. Civ. Code § 1798.82(b),
16 Plaintiff and California Subclass members suffered incrementally increased
17 damages separate and distinct from those simply caused by the data breach itself.

18 330. Plaintiff and California Subclass members seek all remedies available
19 under Cal. Civ. Code § 1798.82(b), including but not limited to the damages
20 suffered by Plaintiff and California Subclass members as alleged above, and
21 equitable relief.

22 **RELIEF REQUESTED**

23 Plaintiffs, on behalf of all others similarly situated, request that the Court
24 enter judgment against Defendants including the following:

- 25 A. Determining that this matter may proceed as a class action and
- 26 certifying the Classes asserted herein;
- 27 B. Appointing Plaintiffs as representatives of the applicable Classes and
- 28 appointing Plaintiffs’ counsel as Class counsel;

- 1 C. An award to Plaintiffs and the Classes of compensatory,
- 2 consequential, nominal, statutory, and treble damages as set forth
- 3 above;
- 4 D. Ordering injunctive relief requiring Defendants to, among other
- 5 things: (i) strengthen its data security systems and monitoring
- 6 procedures; (ii) submit to future annual audits of those systems; (iii)
- 7 provide several years of free credit monitoring and identity theft
- 8 insurance to all Class members; and (iv) timely notify consumers of
- 9 any future data breaches;
- 10 E. Entering a declaratory judgment stating that Defendants owe a legal
- 11 duty to secure consumers’ e-PHI, to timely notify patients of any data
- 12 breach, and to establish and implement data security measures that are
- 13 adequate to secure patients’ e-PHI;
- 14 F. An award of attorneys’ fees, costs, and expenses, as provided by law
- 15 or equity;
- 16 G. An award of pre-judgment and post-judgment interest, as provided by
- 17 law or equity; and
- 18 H. Such other relief as the Court may allow.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

22 Dated: December 10, 2021

/s/ Ronald A. Marron
 Ronald A. Marron (175650)
 Alexis M. Wood (270200)
 Kas L. Gallucci (288709)
 Lilach Halperin (323202)
**LAW OFFICES OF RONALD A.
 MARRON**
 651 Arroyo Drive
 San Diego, CA 92103

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Tel: (619) 696-9006
Fax: (619) 564-6665
ron@consumersadvocates.com
alexis@consumersadvocates.com
kas@consumersadvocates.com
lilach@consumersadvocates.com

Christian Levis (pro hac vice forthcoming)
Amanda Fiorilla (pro hac vice forthcoming)
Rachel Isabel Kesten (pro hac vice
forthcoming)

LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com
rkesten@lowey.com

Anthony M. Christina (pro hac vice
forthcoming)

LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Fax: (914) 997-0035
achristina@lowey.com

*Attorneys for Plaintiffs and the Proposed
Classes*