STEPHEN R. BASSER (121590)
sbasser@barrack.com
SAMUEL M. WARD (216562)
sward@barrack.com
BARRACK, RODOS & BACINE
One America Plaza
600 West Broadway, Suite 900
San Diego, CA 92101
Phone: (619) 230–0800
Fax: (619) 230–1874

Attorneys for Plaintiffs
(Additional Counsel for Plaintiffs Appear on Signature Page)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

V.K., T.R., and J.S., individually, and on behalf of all others similarly situated, Plaintiffs, v. BETTERHELP, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs V.K., T.R., and J.S., acting anonymously to safeguard their identities, bring this action on behalf of themselves and all others similarly situated (the "Class Members") against BetterHelp, Inc. ("BetterHelp" or "Defendant"). The allegations contained in this Class Action Complaint are based on Plaintiffs' personal knowledge of facts pertaining to themselves, and upon information and belief as to all other matters, including upon information and belief with respect to allegations derived from an investigation conducted by the United States Federal Trade Commission.

INTRODUCTION

1. This is a class action brought on behalf of a nationwide class to address Defendant's improper, unauthorized, and illegal disclosure of the personally identifiable information ("PII") and/or the protected health information ("PHI") (PII and PHI are collectively referred to as "Private Information") of Plaintiffs and Class Members to third-party advertising platforms, including Facebook and others.

2. BetterHelp, a telehealth company based in California, operates through various websites. It claims to be the "world's largest therapy platform," describing itself as a "mental health platform that provides online mental health services directly to consumers" which are "provided through web-based interaction, as well as phone and text communication." Defendant developed, advertised, and offered for sale and sold an online mental health counseling service matching users with BetterHelp's therapies, and then facilitated counseling via its websites.

3. At all times material, BetterHelp has offered mental health services under a variety of business names, as more fully alleged hereafter, providing those services to Class Members who pay a price premium for maintaining confidentiality of their Private Information. BetterHelp has reportedly served over one million patients nationwide over the last several years, and within the Class Period, as defined below.

4. Information about a person's mental health is unquestionably highly confidential, sensitive information pertaining to an individual. Disclosing the fact that someone has even sought mental health services can engender adverse consequences for that person, including

discrimination in the workplace, social ostracization, and even denial of insurance coverage. Individuals seeking mental health services necessarily trust that their Private Information and, in particular, the fact that they have sought mental health therapy or consultation, will be kept private and confidential. Absent such confidentiality and privacy, many people would be deterred from or certainly less likely to seek mental health related treatment, thereby potentially leading to more serious problems.

5. The United States Department of Health and Human Services ("HHS") has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how healthcare providers must safeguard and protect Private Information. Under this Privacy Rule, and pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), no healthcare provider is permitted to disclose personally identifiable or protected health information of an individual or patient to a third party without that individual's or patient's express written authorization.

6. The Federal Trade Commission ("FTC") conducted an investigation of BetterHelp and, according to a complaint that the FTC filed on March 7, 2023, which is a matter of public record, found by virtue of its investigation, and as it alleged, that Defendant continuously broke promises to protect consumers' Private Information during the period from 2013 to and including December 2020. While flagrantly doing so, BetterHelp actually used their Private Information to target existing and new customers with advertising for its services, while disseminating or otherwise disclosing Class Members' Private Information to some of the largest online advertising companies in the world, including Facebook, Pinterest, and SnapChat, thereby enabling those third-parties to exploit for profit sensitive Private Information.

7. Samuel Levine, the Director of the Bureau of Consumer Protection of the Federal Trade Commission, has underscored the fact that "[D]igital health companies and mobile apps should not cash in on consumers' extremely sensitive and personally identifiable health information," while noting that the sale of this information constitute blatent "misuse and illegal exploitation."

8. Nonetheless, rather than protecting Plaintiffs' and Class Members' confidential and sensitive Private Information, Defendant installed web beacons and cookies on its websites to track consumer Class Members and collect data and information about them that it could later monetize and/or that third parties could monetize to whom it transmitted such confidential health related information.

9. While it flagrantly disregarded Plaintiffs' and other Class Members' privacy rights by intentionally, willfully, and recklessly failing to take the necessary precautions required to safeguard and protect their PHI and PII from unauthorized disclosures, Defendant improperly handled, failed to protect, and readily enabled third parties to copy, intercept or receive such Private Information.

10. Defendant failed to employ reasonable measures to safeguard Private Information it collected from consumers, failed to properly train its employees to protect Private Information when using it for advertising, failed to properly supervise staff in the use of Private Information, failed to provide consumers with proper notice as to the collection, use, and disclosure of their Private Information, and failed to limit how third parties could use consumers' Private Information.

11. Defendant's wrongful actions and/or inactions, and resulting breach of duty, have placed Plaintiff and other Class Members in imminent, immediate, and continuing increased risk of identity theft, identity fraud and medical fraud, while also exposing the fact that they sought mental health services, thereby potentially stigmatizing them, and even prejudicing their ability to be gainfully employed or secure employment or other positions.

12. Plaintiffs and Class Members have also suffered damages for the loss of the benefit of their bargain with Defendant, including having paid a price premium for its services, which included the protection of their Private Information. In that regard, Plaintiffs and Class Members paid more for privacy and confidentiality than they otherwise would have, and paid for privacy protection they did not receive, consequently being damaged by virtue of the fact that they did not receive the benefit of their bargain, and have suffered an ascertainable loss.

13. Defendant's actions constitute an extreme invasion of Plaintiff and Class members' right to privacy and violate several statutory and common law doctrines, including the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631, *et seq.*; the California Constitution Article I, Section I; California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.*; California's Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq.*; California's Online Privacy Protection Act, California Business and Professions Code §§ 22575-22579 ("CalOPPA"); the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq.* ("FTC Act"), the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Parts 160 and 164; and common law doctrines such as breach of implied contracts, breach of fiduciary duty and breach of confidence.

14. Consequently, Plaintiff brings this action for legal and equitable remedies to address and rectify the illegal and wrongful conduct, and misconduct and actions described herein committed by BetterHelp and those within the scope of its employment and agency.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

16. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and many of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

17. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

DIVISIONAL ASSIGNMENT

18. Pursuant to Civil Local Rule 3-2(c), a substantial part of the events giving rise to the claims brought in this Complaint occurred in Santa Clara County, California. Consequently, assignment of this action to the San Jose Division is appropriate.

THE PARTIES

Plaintiffs

19. Plaintiff V.K. is an adult citizen of the State of California who accessed a BetterHelp site and is bringing this action anonymously to protect her confidential Private Information, which is protected under HIPAA, and seek redress.

20. Plaintiff T.R. is an adult citizen of the State of California who accessed a BetterHelp site and is bringing this action anonymously to protect his confidential Private Information, which is protected under HIPAA, and seek redress.

21. Plaintiff J.S. is an adult citizen of the State of California who accessed a BetterHelp site and is bringing this action anonymously to protect her confidential Private Information, which is protected under HIPAA, and seek redress.

Defendant

22. Defendant BetterHelp, Inc., also doing business as Compile, Inc.; MyTherapist; Teen Counseling; Faithful Counseling; Pride Counseling; iCounseling; ReGain; and Terappeuta, is a Delaware corporation with its principal office or place of business located at 990 Villa St., Mountain View, CA. BetterHelp operates in and from California through the website https://BetterHelp.com/. The Company services millions of patients nationwide. According to the FTC: "Since BetterHelp was founded, more than two million people have signed up, entrusting the company with their Private Information, much of it related to the status of their health – and their mental health."

23. Through the wrongful conduct at issue herein, BetterHelp has allowed companies like Meta, Snapchat, and Pinterest to surreptitiously collect user data such as provided by Plaintiffs and others, and associate it with Class Members' Facebook and other accounts for use in targeting them with advertisements. This private information was also used to target other individuals for advertising and to increase the profits of BetterHelp and third party social media companies.

24. Defendant is a covered entity pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). See 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. See 45 C.F.R. Part 160 and Part 164, Subparts A through E. Defendant is also a covered entity pursuant to the Health Information Technology Act ("HITECH")[1] . See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

25. The HIPAA and HITECH rules work in conjunction with the already established laws of privacy in California. HIPAA and HITECH do not recognize an individual right of claim for violation, but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

26. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

FACTUAL ALLEGATIONS

Background Regarding BetterHelp Services and Business

27. BetterHelp serves the public through a primary website and app and via other related websites and apps. It has been in operation since 2013, and includes related entities, Faithful Counseling. Pride Counseling. Teen Counseling and ReGain. BetterHelp and its related sites function similarly, facilitate therapy and are all subject to BetterHelp policies, practices, and procedures.[2]

28. BetterHelp users pay $60 to $90 per week for counseling after signing up for the service. Upon visiting one of the sites a user must fill out a questionnaire (the "Intake Questionnaire"), answering detailed questions about his or her mental health, after which the user is prompted to create an account for the service by entering his or her name or nickname, email address, phone number, and emergency contact information, and enter credit card information.

---

[1] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

[2] BetterHelp also offers its service through the iCounseling website and app, the Terappeuta website and app, and the MyTherapist website and app.

29. BetterHelp then utilizes the user's responses to the Intake Questionnaire to match the user with one of its more than 25,000 licensed therapists who thereafter provide them with mental health therapy via video conferencing, text messaging, live chat, and audio calls.

30. BetterHelp's primary website and app, called "BetterHelp," has enjoyed considerable growth, adding over 118,000 U.S. Users in 2018, over 158,000 U.S. Users in 2019, and over 641,000 U.S. Users in 2020. Since its inception, BetterHelp has signed up over 2 million Users, earning over $345 million in revenue in 2020, and over $720 million in revenue in 2021.

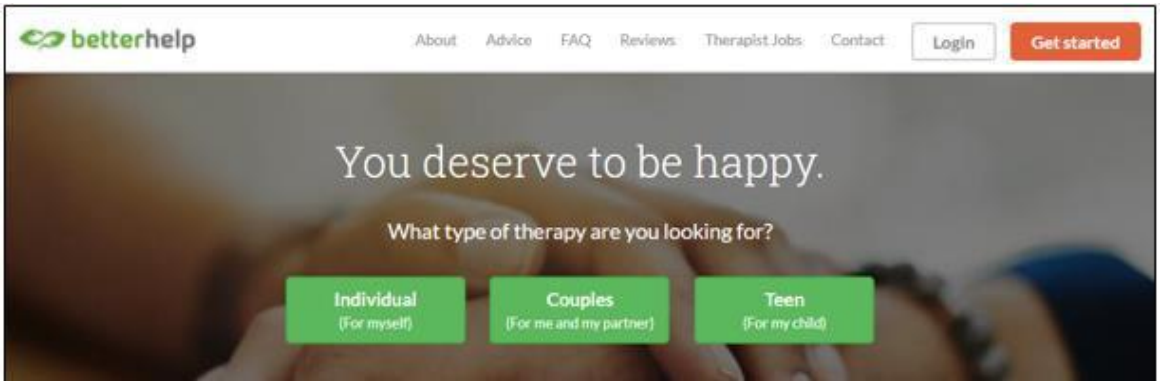
BetterHelp's Deceptive Marketing and Business Practices

31. BetterHelp has historically utilized numerous third parties to market its services, including, Facebook, Snapchat, Pinterest, and Criteo. In addition, it has advertised its service on search engines, television, podcasts, and radio, spending millions of dollars annually for marketing. In 2020, for example, it spent $10-$20 million on Facebook advertising. By 2021, its advertising on Facebook was bringing in approximately 30,000 to 40,000 new Users per quarter.

32. In connection with the advertisement and sale of its services, Defendant has disseminated, or caused to be disseminated, false and deceptive statements about its use and disclosure of consumers' health information, along with misleading and deceptive representations regarding its compliance with federal health privacy laws, thereby misleading users.

A. Deceptive Statements About Privacy on Respondent's Websites and Apps

33. Upon arriving at any of the BetterHelp related sites, a user is immediately prompted to fill out an Intake Questionnaire. For example, on the BetterHelp website, a Visitor begins the Intake Questionnaire by selecting whether he or she is looking for "Individual," "Couples," or "Teen" therapy, as shown below:



34. After making a selection, the Intake Questionnaire asks several questions, including whether the user is "experiencing overwhelming sadness, grief, or depression"; has been having thoughts that he or she "would be better off dead or hurting yourself in some way"; is "currently taking any medication," has "problems or worries about intimacy"; and whether the user has previously been in therapy.

35. BetterHelp included privacy assurances throughout the Intake Questionnaire. Until November 2021, each site displayed a banner at the top of each question, explaining that Defendant is merely asking for "some general and *anonymous* background information about you and the issues you'd like to deal with in online therapy" (emphasis added) so that the user can be matched "with the most suitable therapist for you."

36. The Intake Questionnaire includes additional periodic privacy assurances. From at least August 2017 to December 2020, when a user reached the question as to whether he or she was taking medication, the user was shown the statement: "Rest assured—any information provided in this questionnaire will stay private between you and your counselor." In December 2020, BetterHelp changed that statement to read: "Rest assured—*this information* will stay private between you and your counselor" (emphasis on alteration added). Then, in January 2021, it was changed again to state: "Rest assured—*your health information* will stay private between you and your counselor" (emphasis on alteration added), as illustrated and circled below:

In October 2021, BetterHelp completely removed this representation.

37. After being presented with these repeated promises of privacy, millions of visitors to the sites, including those that became users, filled out the Intake Questionnaire and shared their health information with Defendant.

38. Nonetheless, and contrary to its assurances of privacy, Defendant disclosed users' Intake Questionnaire responses, as well as their email addresses and IP addresses, to Facebook for advertising purposes, as well as for Facebook's own purposes, as more fully discussed below.

39. Between August 2017 and December 2020, Defendant gave additional privacy assurances to Faithful Counseling, Pride Counseling, and Teen Counseling users as inducement to sign up for its service that their email addresses would be "kept strictly private" and "never shared, sold or disclosed to anyone," which representation was displayed prominently and unavoidably during the sign-up process.

40. Defendant was aware that any disclosure of user's email addresses in association with BetterHelp revealed that they were seeking mental health treatment: information such consumers wanted along with their identities.

41. Nevertheless, Defendant disclosed the email addresses of thousands of these users to various third parties for advertising purposes and the third parties' own purposes, as more fully discussed below, consequently revealing to the third parties that these consumers and Class Members were seeking and/or receiving mental health treatment via its service.

42. In September 2020, Defendant added the below banner to the bottom of every page of its sites (until a user closed it), stating: "We use cookies to help the site function properly, analyze usage, and measure the effectiveness of our ads. We **never** sell or rent any information you share with us. Read our Privacy Policy [(linked)] to learn more." (Emphasis provided).

43. But despite including a link to the privacy policy, users were effectively dissuaded from reading the privacy policy because, until October 2020, Defendant represented that it would "never sell or rent any information you share with us."

44. In May 2021, the banner was revised to add the following underlined language: "We use BetterHelp and third-party cookies and web beacons to help the site function properly, analyze usage, target and measure the effectiveness of our ads. Read our Privacy Policy [(linked)] to learn more and go to Cookie Preferences to manage your settings" (emphasis added). However, this banner still did not inform Class Members that BetterHelp would use and disclose their health information for advertising or that third parties would be able to use the information for their own purposes.

45. It was not until October 2021 that Defendant revised the banner to state that it discloses IP addresses and other personal identifiers for advertising and offered Class Members an opportunity to opt out of the disclosures via the banner.

46. Defendants privacy policy made additional deceptive statements regarding the use and disclosure of health information. For example, from August 2013 to November 2018, Defendants privacy policies represented that it would use and disclose consumer Class Members' email addresses, IP addresses, enrollment in the service, and Intake Questionnaire responses for **certain** purposes, including to connect them with therapists and operate the service, but made no mention of using or disclosing this information for advertising purposes, or permitting third parties to use this information for their own purposes.

47. In November 2018, Defendant updated the privacy policy to state affirmatively that it would use and disclose this information **only** for limited purposes, such as to operate and improve the service, which limited purposes did not include using or disclosing the information for advertising or disclosing the information to third parties for their own purposes.

48. Defendant revised its privacy policy again in September 2019, stating that it might *use* this health information for advertising, but would only *disclose* this information to third parties for **certain** stated **limited purposes**, **which did not include advertising or the third parties' own purposes**. In September 2020, Defendant again revised the privacy policy, finally stating that it may *both use and disclose* Class Members' information for advertising. Still, the privacy policy continued to claim that BetterHelp would only disclose this information to third parties for only the stated limited purposes, which did not include third parties' own purposes.

49. From August 2013 to June 2021, Respondent's privacy policies stated that it would use web beacons (including pixels) and cookies for limited purposes. These limited purposes did not include the use or disclosure of health information for advertising purposes, or the disclosure of this information for third parties' own purposes.

50. But, as more fully discussed below, these privacy policy representations were misleading. In truth, Defendant used and disclosed health information for advertising purposes and disclosed this information to third parties for their own purposes, from 2013 to December 2020, and through various means, including by uploading consumers' email addresses to third-party advertising platforms, and through web beacons (specifically pixels) it had placed on various pages of its related sites.

B. BetterHelp's Use and Disclosure of Millions of Consumers' Health Information for Advertising

51. Defendant repeatedly broke each of its aforementioned privacy promises since 2013, using email addresses, IP addresses, enrollment in the service, and certain Intake Questionnaire responses for various advertising purposes, including (1) re-targeting consumer

Class Members with advertisements for the service; (2) using consumer Class Members' health information to secure and target potential new users with advertisements; and (3) optimizing Defendant's targeting advertisements at individuals. Defendant utilized a number of third-party advertising platforms, including Facebook, Snapchat, Criteo, and Pinterest, to carry out this advertising. As a consequence of using this health information for advertising, BetterHelp has secured hundreds of thousands of new users, including consumer Class Members, resulting in many millions of dollars in additional revenue.

52. Each such disclosure of a consumer Class Member's email address constituted a disclosure of their health information, and because it was collected only from consumers seeking mental health therapy via the service (by filling out the Intake Questionnaire, signing up for the service, and/or becoming a user), disclosure of their email address implicitly identified the visitor or user as one seeking and/or receiving mental health treatment via the service.

53. Between 2017 and 2018, Defendant uploaded lists of over 7 million such email addresses to Facebook, and Facebook matched over 4 million of these consumer Class Members with their Facebook user IDs, linking their use of the service for mental health treatment with their Facebook accounts. Some examples are:

a. January 2017 – October 2018: Uploading over 170,000 consumer Class Members' email addresses to Facebook, re-targeting these individuals and targeting potential new users with advertisements for the service.

b. January 2018 – October 2018: Uploading over 15,000 users' email addresses to Facebook to find and target new potential Users with advertisements for the service.

c. October 2017: Uploading the email addresses of all their current and former users—nearly 2 million in total—to Facebook, targeting them all with advertisements to refer their Facebook friends to the service.

54. From 2013 to December 2020, Defendant shared consumer Class Members' email addresses, IP addresses, and records known as "Events" with Facebook. These Events automatically tracked certain of their actions so that information with the consumer Class Members Facebook accounts for advertising. Some examples are:

a. January 2018: BetterHelp disclosed to Facebook that over 70,000 consumers had signed up for accounts (but had not become paying users)—through an Event denoting as much—in order to re-target them with advertisements for the service.

b. November 2018 – March 2020: BetterHelp disclosed to Facebook over 1.5 million consumer Class Members' previous therapy—gathered through their affirmative responses to the Intake Questionnaire question "Have you been in counseling or therapy before?"—to re-target them with advertisements and optimize its own advertisements.

c. October 2018 – November 2020: BetterHelp used and shared over 3.5 million consumer Class Members "good" or "fair" financial status—gathered through the Intake Questionnaire—with Facebook to optimize its advertisements and to find potential new Users and target them with advertisements.

d. January – December 2020: BetterHelp shared with Facebook the fact that over 180,000 consumers had become paying users—through an Event denoting they had entered credit card information after completing the Intake Questionnaire—to optimize its advertisements and to find potential new users and target them with advertisements.

55. In January 2019, Defendant disclosed to Snapchat the IP addresses and email addresses of approximately 5.6 million consumers visiting its sites to re-target them with advertisements for its service. From July 2018 to January 2019, Defendant disclosed the email addresses of over 70,000 individuals to Criteo in order to re-target them with advertisements. And, from August 2019 to September 2020, it disclosed consumer Class Members' email addresses to Pinterest for advertising.

C. Failure to Limit Third Parties' Use of Health Information

56. In disclosing consumer Class Members' health information to Facebook and other third parties, BetterHelp did not contractually limit how the third parties could use and disclose the data other than merely agreeing to these third parties' general terms of service, which either placed no restrictions on the third parties' use and disclosure of the information or specifically permitted the third parties to use the information for their own purposes. Facebook has in fact used the consumer Class Members' information it received from BetterHelp for its own purposes, including improving its advertising products, tracking suspicious activity on its platforms, and research and development.

D. BetterHelp's Deceptive Statements Were Material

57. BetterHelp's deceptive privacy assurances were material to consumer Class Members, as they want to keep their health information private, especially in the context of therapy. Plaintiffs are further informed and believe and thereupon allege that Defendant's own service representatives inform consumers that their "name, age, address, *email*, *medical history*, conversations between you and your counselor" are "PHI" or "Protected Health Information"[2] (emphasis added).

E. Respondent's Deceptive HIPAA Seal

58. From September 2013 to December 2020, BetterHelp displayed seals — implying its purported compliance with HIPAA. These seals are circled in red below:

September 2013 – December 2015:

January 2016 – December 2020:

59. By displaying the HIPAA seals, Defendant signaled to consumers that a government agency or other third party had determined that its security practices met HIPAA's requirements. But no government agency or other third party reviewed Defendant's information practices for compliance with HIPAA, let alone determined that the practices met the requirements of HIPAA. Nonetheless, Defendant represented to consumers that it was in fact HIPAA certified.

60. In December 2020, after receiving a Civil Investigative Demand from the U.S. Federal Trade Commission, Defendant removed the "HIPAA" seals from is sites.

F. Defendant's Privacy Practices Failed to Safeguard Confidential HIPAA Protected Information, Injuring Consumers

61. From at least 2017 to at least 2021, Defendant engaged in a number of practices that, individually or taken together, failed to safeguard consumer Class Members' health information with respect to the collection, use, and disclosure of that information. For example, Defendant:

a. failed to develop, implement, or maintain written organizational standards, policies, procedures, or practices with respect to the collection, use, and disclosure of consumers' health information, including ensuring that Respondent's practices complied with its privacy representations to consumers;

b. failed to provide adequate guidance or training for employees or third-party contractors concerning properly safeguarding the privacy of consumers' health information in connection with the collection, use, and disclosure of that information;

c. failed to properly supervise employees with respect to their collection, use, and disclosure of consumers' health information;

d. failed to obtain consumer Class Members' affirmative express consent to collect, use, and disclose their health information for its advertising, as well as for third parties' own purposes, such as research and improvement of their own products; and

e. failed to contractually limit third parties from using consumer Class Members' health information for their own purposes, including but not limited to research and improvement of their own products, when it did not provide them notice or obtain their consent for such uses.

62. Defendant misrepresented its practices with respect to its collection, use, and disclosure of consumer Class Members' health information, and failed to provide them with adequate notice or obtain their consent as to these practices, all the while disclosing health information to numerous third parties without authorization.

63. Until no earlier than January 2021, BetterHelp did nothing to ensure that its collection, use, and disclosure practices complied with their privacy promises.

64. Defendant's unfair and deceptive acts and practices were violative of Section 5 of the Federal Trade Commission Act, 18 U.S.C. § 45(a).

G. Injury to Consumer Class Members

65. BetterHelp's collection, use, and disclosure of millions of consumer Class Members' health information without reasonable privacy practices or safeguards has caused or is likely to cause them substantial injury. This health information is highly sensitive, and its disclosure without authorization shall likely to cause them stigma, embarrassment, and emotional distress, and especially since it can affect their ability to obtain and/or retain employment, housing, health insurance, or disability insurance.

66. In addition, users pay $60 to $90 per week for the service, which provides mental health therapy and counseling and includes privacy as an integral component—a price that includes a "price premium" based on BetterHelp's deceptive privacy assurances. Had Defendant not made these deceptive claims, consumers would not have been willing to purchase a subscription at the prevailing price because of consumers' privacy concerns. Thus, Defendant's deceptive privacy claims enabled it to inflate the price it charged to consumers, whose actual willingness to pay would have been lower had they known about the true privacy issues concerning its services. Consumers have therefore been injured by having to pay this price premium.

Defendant Violated HIPAA Standards

67. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[3]

68. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

69. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards

[3] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

for the protection of health information that is held or transferred in electronic form. See 42 C.F.R. §§ 164.302-164.318.

70. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. See 45 C.F.R. § 164.530(c).

71. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. See 45 C.F.R. § 164.530(e).

72. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. See 45 C.F.R. § 164.530(f).

73. Under HIPAA:

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.[4]

74. HIPAA and HITECH obligated Defendant to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that

[4] 45 C.F.R. § 160.103

had been granted access rights and who have a working need to access and view the information. See 45 C.F.R. § 164.312(a)(1); see also 42 U.S.C. §17902.

75. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. See 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); see also 42 U.S.C. §17902.

76. HIPAA further obligated Defendant to ensure that its workforce complied with HIPAA security standard rules (see 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. See 45 C.F.R. § 164.530(b)(1).

77. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. See 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." See US Department of Health & Human Services, Security Rule Guidance Material.3 The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represents the industry standard for good business practices with respect to standards for securing e-PHI." See US Department of Health & Human Services, Guidance on Risk Analysis.4

78. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to

determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

> (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);
>
> (2) the recipient of the PHI;
>
> (3) whether the PHI was actually acquired or viewed; and
>
> (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."5

79. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

80. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train its employees and staff so that all its staff and employees know their rolls in facility security.

81. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[5]

82. In its guidance for Marketing, the Department further instructs: The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule

---

[5] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/Deidentification/hhs_deid_guidance.pdf (last visited April 5, 2023).

requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).[6]

83. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[7]

84. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

85. In other words, HHS has expressly stated that Defendant has violated HIPAA Rules.

IP Addresses Are Personally Identifiable Information

86. On information and belief, Defendant also disclosed and sold Plaintiffs' and Class Members' computer IP addresses.

87. An IP address is a number that identifies the address of a device connected to the Internet.

88. IP addresses are used to identify and route communications on the Internet.

89. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

90. Under HIPAA, an IP address is considered personally identifiable information:

---

[6] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited April 5, 2023)

[7] See https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited April 5, 2023).

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. See 45 C.F.R. § 164.514 (2).
- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); See also, 45 C.F.R. § 164.514(b)(2)(i)(O).

91. Consequently, by disclosing IP addresses, Defendant's business practices further violated HIPAA and industry privacy standards.

Defendant Violated Industry Standards

92. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

93. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

94. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, personal data (informational privacy)

95. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive Private Information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

96. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must…: (c) release patient information only in keeping ethics guidelines for confidentiality.

97. Defendant's business practices violated these medical industry standards.

Plaintiffs' and Class Members' Expectation of Privacy

98. Plaintiffs and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

99. Indeed, at all times when Plaintiffs and Class Members provided their PII and PHI to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

CLASS ALLEGATIONS

81. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure individually and on behalf of the following Class:

> All natural persons in the United States whose PII, PHI, or Private Information was collected through BetterHelp websites through third party on-line tracking codes since August 1, 2017.

82. The Class Period is defined as beginning with the date established by the Court's determination of any applicable statute of limitations and after consideration of any tolling, concealment, or accrual issues. The Class Period is defined as ending with the the date of entry of judgment in this action.

83. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

84. **Numerosity/Ascertainability**: While the exact number of members of the Class is unknown at this time, Plaintiffs are informed and believe and thereupon allege that the number

of persons affected by Defendant's conduct is in the tens, if not hundreds of thousands, making joinder of each individual Class Member impracticable. Ultimately, members of the Class will be easily identified through Defendant's records as well as those of third parties.

85. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether and to what extent Defendant had a duty to protect Plaintiffs' and Class Members' Private Information;

b. Whether Defendant had duties not to disclose the Plaintiffs' and Class Members' Private Information to unauthorized third parties;

c. Whether Defendant had duties not to use Plaintiffs' and Class Members' Private Information for non-healthcare purposes;

d. Whether Defendant had duties not to use Plaintiffs' and Class Members' Private Information for unauthorized purposes;

e. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' Private Information;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether Defendant failed to properly implement and configure the tracking software on its digital platforms to prevent the unauthorized use or disclose of Private Information;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the unauthorized disclosure of Private Information to occur; and

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiffs' and Class Members' Private Information.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

86. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

87. Plaintiffs and Class Members were required to submit Private Information to healthcare providers, including Defendant, in order to obtain insurance coverage and/or to receive healthcare services.

88. Defendant knew, or should have known, of the risks and responsibilities inherent in collecting and storing the Private Information of Plaintiffs and Class Members.

89. As described above, Defendant owed duties of care to Plaintiffs and Class Members whose Private Information had been entrusted to Defendant.

90. Defendant breached its duties to Plaintiffs and Class Members by failing to secure their Private Information from unauthorized disclosure to third parties.

91. Defendant acted with wanton disregard for the security of Plaintiffs and Class Members' Private Information.

92. A "special relationship" exists between Defendant and the Plaintiffs and Class Members. Defendants entered into a "special relationship" with Plaintiffs and Class Members because they collected and/or stored the Private Information of Plaintiffs and the Class Members.

93. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiffs and the Class Members, Plaintiffs and the Class Members would not have been injured.

94. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known they were failing to meet their duties, and that Defendant's breach would of such duties cause Plaintiffs

and Class Members to experience the foreseeable harms associated with the unauthorized exposure of their Private Information.

95. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

96. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

97. Pursuant to HIPAA (42 U.S.C. §1302d, *et seq.*), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

98. Defendant breached its duties to Plaintiffs and Class Members under HIPAA (42 U.S.C. § 1302d, *et seq.*), by failing to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information, *i.e.*, by affirmatively sharing Plaintiffs' and Class Members' Private Information, without their authorization, with third parties.

99. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

100. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

101. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that they were failing to meet its duties, and that Defendant's breach of those duties would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the unauthorized sharing of their Private Information.

102. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On behalf of Plaintiffs and the Class)

103. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

104. Plaintiffs and Class members entered into an implied contract with Defendant when they obtained or purchased healthcare related services from Defendant and/or their affiliated healthcare providers, and for which they provided their Private Information. The Private Information provided by Class Members that was collected and stored by Defendant was governed by and subject to privacy duties and policies.

105. Defendant implicitly and/or expressly agreed and was under a duty to safeguard and protect the Private Information of Plaintiffs and Class Members from disclosure.

106. Plaintiffs and Class members entered into the implied contracts with the reasonable expectation that Defendant's privacy security practices and policies were reasonable and consistent with industry standards. Plaintiffs and Class members believed that Defendant would use part of the monies paid to Defendant under the implied contracts to fund adequate and reasonable security practices maintaining the confidentiality of their Private Information.

107. Plaintiffs and Class members would not have obtained healthcare services from Defendant or their affiliated healthcare providers or entrusted their Private Information which was provided to and stored by Defendant in the absence of the implied contract or implied terms between them and Defendant and its affiliated healthcare providers. The safeguarding of the Private Information of Plaintiffs and Class Members was critical to realize the intent of the parties.

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

109. Defendant breached its implied contracts with Plaintiffs and Class members to protect their Private Information when Defendant disclosed the Private Information collected to unauthorized third parties while failing to notify Plaintiffs and the Class that Defendant were so doing.

110. As a direct and proximate result of Defendant's breaches of implied contract, Plaintiffs and Class members sustained actual losses and damages as described in detail above, and are also entitled to recover nominal damages.

COUNT IV
Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the Class)

111. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

112. Plaintiffs and Class Members entered into valid, binding, and enforceable express or implied contracts with Defendant, as alleged above.

113. The contracts respecting which Plaintiffs and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendant would act fairly and in good faith in carrying out their contractual obligations to take reasonable measures to protect Plaintiffs' Private Information from unauthorized disclosure and to comply with state laws and regulations.

114. A "special relationship" exists between Defendant and the Plaintiffs and Class Members. Defendant entered into a "special relationship" with Plaintiffs and Class Members who sought medical services or treatment and, in doing so, entrusted Defendant, with their Private Information.

115. Despite this special relationship with Plaintiffs, Defendant did not act in good faith and with fair dealing to protect Plaintiffs' and Class Members' Private Information.

116. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant.

117. Defendant's failure to act in good faith in complying with the contracts denied Plaintiffs and Class Members the full benefit of their bargain, and instead they services that were less valuable than what they paid for and less valuable than their reasonable expectations.

118. Accordingly, Plaintiffs and Class Members have been injured as a result of Defendant's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

119. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations as if fully set forth herein.

120. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and do store.

121. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship with its patients, in particular, to keep secure their Private Information from disclosure without authorization from Plaintiffs and the Class Members.

122. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to notify and/or warn Plaintiffs and Class Members that Defendant was sharing their Private Information with third parties.

123. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

124. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the compromise and sharing of their Private Information; and (ii) the diminished value of the services they received.

125. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
Breach of Duty
(On behalf of Plaintiffs and the Class)

126. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

127. Defendant accepted the special confidence placed in them by Plaintiffs and Class Members. There was an understanding between the parties that healthcare service provider Defendant would act for the benefit of Plaintiffs and Class Members in preserving the confidentiality of their Private Information.

128. Defendant became the guardian of Plaintiffs' and Class Members' Private Information and accepted a duty to act primarily for the benefit of its patients, including Plaintiffs and the Class Members, including safeguarding Plaintiffs' and the Class Members' Private Information.

129. Defendant's duty to act for the benefit of Plaintiffs and Class Members pertains as well to matters within the scope of Defendant's healthcare relationship with its patients, in particular, to keep secure the Private Information of those patients.

130. Defendant breached its duties to Plaintiffs and Class Members by (a) sharing their Private Information with third parties without authorization; (b) by failing to notify Plaintiffs and the Class Members that Defendant was doing so; and (c) by otherwise failing to safeguard Plaintiffs' and the Class Members' Private Information.

131. As a direct and proximate result of Defendant's breaches of its duties, Plaintiffs and/or Class Members have suffered and/or will suffer injury, including but not limited to: (a) the compromise of their Private Information; and (b) the diminished value of the services they received as a result of Defendants' unauthorized sharing of Plaintiffs' and Class Members' Private Information and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VII
Violation of the California Invasion of Privacy Act ("CIPA")
California Penal Code §§ 630, 631, and 632, *et. seq.*
(On Behalf of Plaintiffs and the Class)

132. Plaintiffs, on behalf of the Class, re-allege all of the foregoing allegations as if fully set forth herein.

133. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630. The Act bars, and establishes penalties for both the interception and recording of private communications.

134. Cal. Penal Code § 631(a) provides for the imposition of a fine of up to $2,500 for:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable . . . .

135. Cal. Penal Code § 632(a) provides, in pertinent part:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars . . . .

136. A defendant must show it had the consent of all parties to a communication.

137. Defendant, who maintains its principal places of business in California; implemented and effectuated the technology to intercept, track, record, store, transmit, and exploit the aforesaid Private Information while it was engaging in the provision of healthcare services to consumer Class Members.

138. At all relevant times, Defendant's conduct and communications were without authorization and informed consent from the Plaintiffs.

139. The technology implemented by Defendant and related beacon or code constitute an "electronic amplifying or recording device" under the CIPA, the data it collects is exploited for pecuniary gain, and the Private Information constitutes "confidential communications." Plaintiffs and Class members had, at all times material, an objectively reasonable expectation of privacy and confidentiality of their Private Information relating to healthcare services.

140. Plaintiffs have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personally identifiable information.

141. Pursuant to California Penal Code § 637.2, Plaintiffs have been injured by the violations of California Penal Code § 632, *et seq.*, and seeks damages for the greater of $5,000 or three times the amount of actual damages, for each and every instance of violation apiece, and as to Plaintiffs and each Class Member, each of them individually, as well as injunctive relief.

COUNT VIII
Violation of the California Confidentiality of Medical Information Act ("CMIA")
Section 56.10
(On Behalf of Plaintiffs and the Class)

142. Plaintiffs, on behalf of the Class, re-allege all of the foregoing allegations as if fully set forth herein.

143. Pursuant to the California Confidentiality of Medical Information Act § 56.10 ("CMIA"), health care providers are prohibited from disclosing their patients' medical information and information relating to their patients without a patient's authorization. As defined by the CMIA, medical information refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care... regarding a patient's medical history, mental or physical condition, or treatment. 'Individually Identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual..."

144. Plaintiffs and the members of the Class are each patients and Defendant is a health care provider, pursuant to the CMIA. As a healthcare provider, Defendant is obligated to comply with the requirements of the CMIA.

145. As set for the above, the Defendant provides sufficient Private Information and data so as to identify consumers through the collection, sharing, and transmission of, *inter alia*, Private Information.

146. This information is derived from Defendant's provision of health care services to Plaintiffs and the Class, thus, it constitutes medical information pursuant to the CMIA.

147. As set forth above, Defendant failed to get the permission or other valid authorization of Plaintiffs and the Class for disclosure of this healthcare information.

148. As set forth in CMIA § 56.11, a valid authorization for disclosure of medical information must: (1) be "[c]learly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization"; (2) be signed and dated by the patient or his representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date after which the authorization expires. Here, there was no valid authorization.

149. On these facts, Defendant violated CMIA through its disclosure of the Private Information of Plaintiffs and the Class without valid authorization.

COUNT IX
Invasion of Privacy Under California's Constitution
(On Behalf of Plaintiffs and the Class)

150. Plaintiffs, on behalf of the Class, re-allege all of the foregoing allegations as if fully set forth herein.

151. Plaintiffs and the Members of the Class have an interest in protecting and preventing the unauthorized sharing of their Private Information, including their medical information.

152. Plaintiffs and the members of the Class have a further interest in being able to interact with their healthcare providers in a manner that guarantees the confidentiality of the information shared with their health care providers.

153. Plaintiffs and the members of the Class have a further interest in being able to communicate online without fear of their communications being wiretapped or otherwise illicitly shared without their knowledge and authorization.

154. Plaintiffs and Class Members did not authorize Defendant to record and transmit Plaintiffs' and Class Members' Private Information.

155. Defendant's collection, disclosure and sharing, without authorization, of Plaintiffs' and Class Members' Private Information constitutes a serious breach of the Plaintiffs' and the Class Members' respective rights to privacy.

156. Plaintiffs and the members of the Class seek all available relief for Defendant's invasion of their privacy.

COUNT X
Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(On Behalf of Plaintiffs and the Class)

157. Plaintiffs, on behalf of the Class, re-allege all of the foregoing allegations as if fully set forth herein.

158. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201. Defendant violated the California Unfair Competition Law ("UCL"), §§ 17200, *et seq*., by engaging in unlawful, unfair, and deceptive business acts and practices as alleged above by using, and exploiting or divulging to third persons the Private Information of Plaintiffs and Class Members, and without the knowledge of Plaintiffs and the Class intercepting, collecting, using, and exploiting their Private Information.

159. Defendant engaged in unlawful business practices through its numerous violations of law, including violations of California Penal Code §§ 630, 631, and 632, *et seq.*

160. Defendant's aforesaid surreptitious conduct, deception, and omissions respecting Plaintiffs and the Class were material because they were likely to deceive reasonable individuals about Defendant's adherence to their own stated and publicized privacy policies and procedures and their reasonable expectations of the privacy of their Private Information.

161. Defendant's conduct, as described above, was unfair in that it prevented the making of fully informed decisions by consumers, such as Plaintiffs and the members of the Class, which prevented Plaintiffs and the Class from making fully informed decisions regarding the communication of Private Information to their healthcare providers.

162. Defendant intended to deceive or mislead Plaintiffs and the Class, and induced them.

163. Defendant's actions constituted intentional, knowing, and malicious violations of the UCL in reckless disregard of the rights of Plaintiffs and the Class.

164. As a direct and proximate result of Defendant's violations of the UCL, Plaintiffs and the Class sustained actual losses and damages as described herein.

165. Plaintiffs and the Class seek restitution, injunctive relief, and other and further relief as the Court may deem just and proper. To the extent any of these remedies are equitable, Plaintiffs seek them in the alternative to any adequate remedy at law they may have.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, pray for relief and judgment against Defendants as follows:

A. certifying the Class pursuant to Federal Rule of Civil Procedure, Rule 23, appointing Plaintiffs as representatives of the Class, and designating Plaintiffs' counsel as Class Counsel;

B. declaring that Defendant's conduct violates the laws referenced herein;

C. finding in favor of Plaintiffs and the Class on all counts asserted herein;

D. awarding Plaintiffs and the Class compensatory damages and actual damages, trebled, in an amount exceeding $5,000,000, to be determined by proof;

E. awarding Plaintiffs and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiffs and the Class punitive damages;

G. awarding Plaintiffs and the Class civil penalties;

H. granting Plaintiffs and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiffs and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiffs and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

Dated: April 6, 2023

Respectfully submitted,

BARRACK, RODOS & BACINE

/s/ Stephen R. Basser
STEPHEN R. BASSER
SAMUEL M. WARD
600 West Broadway, Suite 900
San Diego, CA 92101
sbasser@barrack.com
sward@barrack.com
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

Andrew J. Heo*
BARRACK, RODOS & BACINE
2001 Market Street, Ste. 3300
Philadelphia, PA 19103
Telephone.: (215) 963-0600
Facsimile: (215) 963-0838
aheo@barrack.com

John G. Emerson*
EMERSON FIRM, PLLC
2500 Wilcrest, Suite 300
Houston, TX 77042
Telephone: (800) 551-8649
Facsimile: (501) 286-4659

Attorneys for Plaintiffs
**pro hac vice* application to be submitted