

1 John J. Nelson (SBN 317598)  
2 **MILBERG COLEMAN BRYSON**  
3 **PHILLIPS GROSSMAN, PLLC**  
4 401 W. Broadway, Suite 1760  
5 San Diego, CA 92101  
6 Telephone: (858) 209-6941  
7 Fax: (865) 522-0049  
8 Email: jnelson@milberg.com

6 Gary. M. Klinger\*  
7 Glen L. Abramson\*  
8 Alexandra M. Honeycutt\*  
9 **MILBERG COLEMAN BRYSON**  
10 **PHILLIPS GROSSMAN, PLLC**  
11 227 W. Monroe Street, Suite 2100  
12 Chicago, Illinois 60606  
13 Telephone: 866.252.0878  
14 Email: gklinger@milberg.com  
15 gabramson@milberg.com  
16 ahoneycutt@milberg.com

12 *Attorneys for Plaintiff*

13 UNITED STATES DISTRICT COURT  
14 FOR THE DISTRICT OF NORTHERN CALIFORNIA  
15 SAN JOSE DIVISION

16 C.M., on behalf of herself and all others  
17 similarly situated,

18 Plaintiff,

19 v.

20 BETTERHELP, INC.,

21 Defendant.

Case No. \_\_\_\_\_

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

1 Plaintiff C.M.<sup>1</sup> bring this class action complaint on behalf of herself and all others similarly  
 2 situated (the “Class Members”) against BetterHelp, Inc. (“BetterHelp” or “Defendant”). The  
 3 allegations contained in this class action complaint are based on Plaintiff’s personal knowledge of  
 4 facts pertaining to herself and upon information and belief, including further investigation conducted  
 5 by Plaintiff’s counsel.

## 6 NATURE OF THE ACTION

7 1. This is a class action lawsuit brought on behalf of a nationwide class to address  
 8 Defendant’s improper, unauthorized, and illegal disclosure of their personally identifiable  
 9 information (“PII”) and/or protected health information (“PHI”) (collectively referred to as “Private  
 10 Information”) to third-party advertising platforms such as Facebook, Snapchat, and others.

11 2. Information about a person’s mental health is among the most confidential and  
 12 sensitive information in our society, and the mishandling of medical information can have serious  
 13 consequences, including discrimination in the workplace or denial of insurance coverage. If people  
 14 do not trust that their medical information will be kept private, they may be less likely to seek  
 15 medical treatment, which can lead to more serious health problems down the road. In addition,  
 16 protecting medical information and making sure it is kept confidential and not disclosed to anyone  
 17 other than the person’s medical provider is necessary to maintain public trust in the healthcare  
 18 system as a whole.

19 3. Recognizing these facts, and in order to implement requirements of the Health  
 20 Insurance Portability and Accountability Act of 1996 (“HIPAA”), the United States Department of  
 21 Health and Human Services (“HHS”) has established “Standards for Privacy of Individually  
 22 Identifiable Health Information” (also known as the “Privacy Rule”) governing how health care  
 23 providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, **no** health  
 24 care provider can disclose a person’s personally identifiable protected health information to a third  
 25 party without express written authorization.

---

26  
 27 <sup>1</sup> Plaintiff brings this action anonymously to protect her confidential personal health information,  
 28 which is protected under the Health Insurance Portability and Accountability Act of 1996  
 (“HIPAA”).

1           4. Defendant has developed, advertised, and offered for sale an online mental health  
2 counseling service that matches users with Defendant’s therapists and then facilitates counseling via  
3 Defendant’s websites, including [www.betterhelp.com](http://www.betterhelp.com), and apps. In addition to general mental health  
4 counseling services, Defendant offers specialized counseling services for specific demographics,  
5 including but not limited to teens (via [www.teencounseling.com](http://www.teencounseling.com)), people of Christian faith (via  
6 [www.faithfulcounseling.com](http://www.faithfulcounseling.com)), and members of the LGBTQ community (via  
7 [www.pridecounseling.com](http://www.pridecounseling.com)). Defendants’ separate websites and apps are collectively referred to  
8 herein as “Defendants’ Website” or the “Website.”

9           5. Millions of consumers have signed up for Defendant’s counseling services. In doing  
10 so, those customers entrusted Defendant with their Private Information, including their health status  
11 and histories, mental health condition, and symptoms and treatment sought, as well as identifying  
12 information such as names, email addresses, and IP addresses.

13           6. Recognizing the sensitivity of this Private Information, Defendant repeatedly  
14 promised to keep it private and use it only for non-advertising purposes such as to facilitate  
15 consumers’ mental health therapy.

16           7. Rather than protecting Plaintiff’s and Class Members’ confidential and sensitive  
17 Private Information, however, Defendant installed web beacons and cookies on its Website to track  
18 users and collect data and information about them that it could later monetize.

19           8. According to a complaint filed by the Federal Trade Commission (“FTC”), from  
20 2013 to December 2020, Defendant continually broke its promises to protect consumers’ Private  
21 Information, instead using it to target existing and new customers with advertising for its services.  
22 Defendant also handed over Plaintiff’s and Class Members’ Private Information to some of the  
23 largest online advertising companies in the world, such as Facebook, Pinterest, Criteo, and Snapchat,  
24 often permitting these companies to use the sensitive Private Information for their own research,  
25 product development, and advertising purposes.

26           9. The FTC also alleged that Defendant: (i) failed to employ reasonable measures to  
27 safeguard Private Information it collected from customers; (ii) failed to properly train its employees  
28 to protect Private Information when using it for advertising; (iii) failed to properly supervise staff

1 in the use of Private Information; (iv) failed to provide customers with proper notice as to the  
 2 collection, use, and disclosure of their Private Information; and (v) failed to limit how third parties  
 3 could use customers' Private Information.

4 10. The FTC's Director of its Bureau of Consumer Protection, Samuel Levine, recently  
 5 stated, "Digital health companies and mobile apps should not cash in on consumers' extremely  
 6 sensitive and personally identifiable health information," noting that the sale of this information  
 7 constituted blatant "misuse and illegal exploitation."

8 11. In response to the use of tracking and data collection technologies by companies  
 9 offering health care services, the Office for Civil Rights at the U.S. Department of Health and  
 10 Human Services ("HHS") recently published a bulletin concerning the Use of Online Tracking  
 11 Technologies by HIPAA Covered Entities and Business Associates (the "Bulletin").<sup>2</sup> The Bulletin  
 12 warns that:

13 An impermissible disclosure of an individual's PHI not only violates the Privacy  
 14 Rule but also may result in a wide range of additional harms to the individual or  
 15 others. For example, an impermissible disclosure of PHI may result in identity theft,  
 16 financial loss, discrimination, stigma, mental anguish, or other serious negative  
 17 consequences to the reputation, health, or physical safety of the individual or to  
 18 others identified in the individual's PHI. Such disclosures can reveal incredibly  
 19 sensitive information about an individual, including diagnoses, frequency of visits to  
 a therapist or other health care professionals, and where an individual seeks medical  
 treatment. While it has always been true that regulated entities may not  
 impermissibly disclose PHI to tracking technology vendors, because of the  
 proliferation of tracking technologies collecting sensitive information, now more  
 than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as  
 expressly permitted or required by the HIPAA Privacy Rule.

20 12. And as recently noted by the Hon. William J. Orrick in a decision concerning the use  
 21 of the data tracking technologies by healthcare organizations, "[o]ur nation recognizes the  
 22 importance of privacy in general and health information in particular: the safekeeping of this  
 23 sensitive information is enshrined under state and federal law."<sup>3</sup>

24 13. Consequently, Plaintiff brings this action for legal and equitable remedies to address  
 25 and rectify the illegal conduct and actions described herein.

26 \_\_\_\_\_  
 27 <sup>2</sup> <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>

28 <sup>3</sup> *In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218, at \*1 (N.D. Cal. Dec. 22, 2022)

**JURISDICTION AND VENUE**

14. 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.

15. 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 Plaintiff's claims occurred in and emanated from this District.

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

**DIVISIONAL ASSIGNMENT**

17. 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**

18. Plaintiff C.M. is an adult citizen of the State of Texas. She brings this action anonymously to protect her confidential personal health information, which is protected under HIPAA.

19. Defendant BetterHelp, Inc. is a Delaware corporation with a principal place of business located at 990 Villa Street, Mountain View, CA 94041.

20. Defendant does business under various other names in addition to BetterHelp, including Compile, Inc., Mytherapist, Teen Counseling, Faithful Counseling, Pride Counseling, Icounseling, Regain, and Terappeuta.

**FACTUAL ALLEGATIONS**

**Background**

21. Defendant BetterHelp has been in operation since 2013, offering online mental health counseling services via various websites and apps.

22. Defendant's primary website, [www.betterhelp.com](http://www.betterhelp.com), offers general counseling services and has been in operation since 2013. In addition, Defendant has numerous other websites and apps that are targeted to more specific demographics. In 2016, Defendant began offering marriage and relationship counseling and services via [www.regain.us](http://www.regain.us). In 2017, Defendant began offering specialized counseling to teenagers via [www.teencounseling.com](http://www.teencounseling.com), to people of Christian faith via [www.faithfulcounseling.com](http://www.faithfulcounseling.com), to the LGBTQ community via [www.pridecounseling.com](http://www.pridecounseling.com).

23. Since its inception, Defendant has signed up over 2 million users and as of 2022 had more than 374,000 active users in the United States. Defendant earned more than \$345 million in revenue in 2020 and more than \$720 million in revenue in 2021.

#### **Defendant's Deceptive and Unfair Marketing Practices**

24. Defendant has spent significant efforts since inception advertising and marketing its services through various digital and traditional media platforms, including television and radio as well as podcasts, search engine ads, and through third parties such as Facebook, Snapchat, Pinterest, and Criteo.

25. Defendant has spent tens of millions of dollars annually to market its counseling services. In 2020, Defendant spent between \$10-20 million on Facebook advertising alone. This advertising was extremely successful; by 2021, Defendant's advertising through Facebook was generating approximately 90,000 – 120,000 new customers per year.

26. Defendant markets all of its services by offering online communications with licensed therapists telling "who you can trust." BetterHelp also claims that customers using its therapists will "get the same professionalism and quality you would expect from an in-office therapist, but with the ability to communicate when and how you want."<sup>4</sup>

---

<sup>4</sup> [betterhelp.com](http://betterhelp.com) (last visited March 6, 2023)

# Professional, licensed, and vetted therapists who you can trust

Tap into the world's largest network of licensed, accredited, and experienced therapists who can help you with a range of issues including depression, anxiety, relationships, trauma, grief, and more. With our therapists, you get the same professionalism and quality you would expect from an in-office therapist, but with the ability to communicate when and how you want.

Get Matched to a Therapist



27. Customers signing up for Defendant’s counseling services pay between \$60 and \$90 per week. To sign up for counseling services, a customer must fill out an online intake questionnaire and answer a detailed series of questions about the customer’s personal life and mental health, including age, gender, marital/relationship status, whether the customer has ever been in therapy before. The online questionnaire also asks questions about the customer’s subjective rating of their physical health, eating habits, financial status, and sleep habits, and the customer’s employment status.

28. The questionnaire also asks a series of questions about symptoms or reasons why the customer is seeking therapy (e.g., feelings of depression, anxiety, grief, etc.), including asking if the customer is “experiencing overwhelming sadness, grief, or depression” or has been having thoughts that the customer “would be better off dead or hurting yourself in some way.”

29. The questionnaire also asks if the customer identifies as religious or as a member of the LGBTQ community, directing them to Faithful Counseling or Pride Counseling, respectively. In addition, teenagers are directed to Teen Counseling.

30. According to the FTC, in 2017, Defendant delegated most decision-making authority over its use of Facebook’s advertising services to a junior marketing analyst who was a recent college graduate, had never worked in marketing, and had no experience and little training in

1 safeguarding consumers' Private Information when using that information for advertising. In 2017  
2 Defendant gave the analyst unilateral authority to decide what Private Information to upload to  
3 Facebook and how to use that information. Defendant provided this marketing analyst with little  
4 training on how to protect customers' Private Information in connection with advertising until 2021.

5 31. Until November 2021, Defendant's Website included privacy assurances throughout  
6 the pages of the questionnaire. For example, at the top of each question, Defendant stated that it was  
7 asking for "general and *anonymous*" background information (emphasis added). In reality, the  
8 information collected was not anonymous.

9 32. In addition, from at least August 2017 to December 2020, Website visitors taking the  
10 questionnaire who reached the question about whether they were taking any medication were shown  
11 the statement: "Rest assured – any information provided in this questionnaire will stay private  
12 between you and your counselor." In December 2020, this statement was changed to read: "Rest  
13 assured – this information will stay private between you and your counselor." In January 2021, the  
14 statement was changed again, reading: "Rest assured – your health information will stay private  
15 between you and your counselor." In October 2021, Defendant removed this representation  
16 altogether.

17 33. Defendant also made false promises about its use of customers' email addresses,  
18 telling visitors to the Faithful Counseling, Pride Counseling, and Teen Counseling websites during  
19 the sign-up process that their email addresses would not be shared. From at least August 2017 to  
20 December 2020, Defendant assured such Website visitors that "Your email address is kept *strictly*  
21 *private*. It is never shared sold or disclosed to anyone. Even your counselor won't know your real  
22 email address." (emphasis added)

23 34. Millions of Website visitors, including those like Plaintiff and Class Members who  
24 ultimately signed up for Defendant's counseling services, were presented with these repeated  
25 promises about the confidentiality of the Private Information they shared with Defendant. Despite  
26 these promises, however, Defendant used Private Information extensively for Defendant's own  
27 profit, including by sharing and disclosing Private Information and selling email addresses.  
28

1           35.     The FTC’s complaint against Defendant sets forth in great detail the extent to which  
 2 Defendant brazenly violated Plaintiff’s and Class Members’ privacy and other rights by disclosing  
 3 Private Information to third parties like Facebook, Snapchat, and others. A copy of the FTC’s  
 4 complaint is attached hereto as Exhibit “A.” A few highlights are worth noting here:

- 5           • The intake questionnaire’s privacy assurances were “displayed in large, high-  
 6 contrast, unavoidable text,” while Defendant’s privacy policies were linked in  
 7 “small, low-contrast writing that is barely visible at the bottom of the page.” When  
 8 Defendant added a banner at the bottom of each page in September 2020  
 9 disclosing its use of cookies, it still falsely stated: “We never sell or rent any  
 10 information you share with us.” Exh. A at 7-9. This was false.
- 11          • Defendant’s privacy policies went through numerous iterations that each  
 12 contained deceptive and misleading statements about Defendant’s use and  
 13 disclosure of Private Information. While Defendant disclosed it would use web  
 14 beacons (including pixels) and cookies for certain limited purposes, it never  
 15 disclosed that it would use or disclose Private Information for advertising  
 16 purposes or to sell to third parties for their own purposes. *Id.* at 9-10
- 17          • Defendant disclosed millions of Class Members’ Private Information to  
 18 advertisers including Facebook. Over 7 million email addresses were uploaded to  
 19 Facebook, which “matched over 4 million of these Visitors and Users with their  
 20 Facebook user IDs, linking their use of the Service for mental health treatment  
 21 with their Facebook accounts.” Defendant also allowed Facebook to  
 22 “automatically track certain actions” of Website users known as “Events.”  
 23 Defendant “recorded and automatically disclosed these Events to Facebook  
 24 through web beacons [Defendant] had placed on each of the [Websites].”  
 25 Defendant and Facebook used this data to target advertising to millions of Class  
 26 Members. *Id.* at 10-12.

27           36.     On March 2, 2023, the FTC announced that it had finalized a Consent Order with  
 28 Defendant addressing Defendant’s deceptive and misleading business practices in using sensitive

1 personally identifiable information and personal health information and disclosing it to third parties.  
2 *See* Exhibit B.

3 37. As part of the Consent Order, Defendant has agreed to pay \$7.8 million to the FTC  
4 and to be subject to various auditing and compliance monitoring procedures in connection with its  
5 privacy policies and handling of customer data and information. *Id.*

6 38. In addition, Defendant is required under the Consent Order to provide its customers  
7 with a Notice advising customers about the FTC action and telling customers that (i) it will tell the  
8 advertising companies that received customers' information to delete it; (ii) it is no longer sharing  
9 customers' health information with other companies for advertising and it is no longer sharing  
10 customers' personal information for advertising without the customers' permission; and (iii) it will  
11 enhance its privacy program to better protect customers' personal health information, including  
12 participating in an independent audit program every two years for the next 20 years. *Id.* at 22-23.

13 **Defendant Was Enriched and Benefitted from the Use and Disclosure of Plaintiff's and Class**  
14 **Members' Private Information, Which Had Financial Value**

15 39. In exchange for disclosing the Private Information of its patients, Defendant was  
16 able to obtain tens or hundreds of thousands of new customers, each of whom paid between \$60 and  
17 \$90 per week for Defendant's counseling services.

18 40. Defendant's disclosure of Private Information also hurt Plaintiff and the Class.  
19 Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user  
20 from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as  
21 high as \$434 per user, for a total of more than \$200 billion industry wide.  
22

23 41. The value of health data in particular is well-known and has been reported on  
24 extensively in the media. For example, Time Magazine published an article in 2017 titled "How  
25 Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the  
26  
27  
28

1 extensive market for health data and observed that the market for information was both lucrative  
2 and a significant risk to privacy.<sup>5</sup>

3 42. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-  
4 identified patient data has become its own small economy: There’s a whole market of brokers who  
5 compile the data from providers and other health-care organizations and sell it to buyers.”<sup>6</sup>  
6

### 7 **IP Addresses Are Personally Identifiable Information**

8 43. On information and belief, Defendant also disclosed and sold Plaintiff’s and Class  
9 Members’ Computer IP addresses.

10 44. An IP address is a number that identifies the address of a device connected to the  
11 Internet.

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

13 46. IP addresses of individual Internet users are used by Internet service providers,  
14 websites, and third-party tracking companies to facilitate and track Internet communications.  
15

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

- 17 • HIPAA defines personally identifiable information to include “any unique  
18 identifying number, characteristic or code” and specifically lists the example of IP  
19 addresses. See 45 C.F.R. § 164.514 (2).
- 20 • HIPAA further declares information as personally identifiable where the covered  
21 entity has “actual knowledge that the information to identify an individual who is a  
22 subject of the information.” 45 C.F.R. § 164.514(2)(ii); See also, 45 C.F.R. §  
23 164.514(b)(2)(i)(O).  
24  
25  
26

---

27 <sup>5</sup> See <https://time.com/4588104/medical-data-industry/> (last visited February 16, 2023).

28 <sup>6</sup> See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited February 16, 2023).

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

### **Defendant Violated Industry Standards**

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

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

51. 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)

52. 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 personal 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.

53. 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.

### **PLAINTIFF'S EXPERIENCE WITH DEFENDANT'S WEBSITE**

54. Beginning in January 2020, Plaintiff C.M. sought counseling services from Defendant to deal with stress and anxiety she was experiencing as the result of serving as a caregiver for her husband, who was critically ill at the time.

1           55. Plaintiff filled out the intake questionnaire and ultimately decided to sign up for  
2 Defendant's services, paying \$130/month for a monthly subscription for psychotherapy and mental  
3 health counseling.

4           56. Prior to deciding to transact with Defendant, Plaintiff viewed and relied upon  
5 Defendant's representations concerning its commitment to maintaining the confidentiality of Private  
6 Information communicated by consumers via Defendant's web platforms. Had Plaintiff known that  
7 Defendant would not maintain her information as private and confidential, Plaintiff would not have  
8 purchased Defendant's services or would have paid less for them.

9           57. Over the next two months, Plaintiff spoke with two BetterHelp therapists to discuss  
10 her mental health issues. Plaintiff's therapy sessions occurred approximately once per week via the  
11 BetterHelp app on her smartphone.  
12

13           58. In December 2021, Plaintiff again sought psychotherapy and mental health  
14 counseling services from Defendant. From December 2021 through March 2022, Plaintiff paid  
15 \$1,005 for numerous live video and telephone therapy sessions with two separate BetterHelp  
16 therapists.  
17

18           59. Beginning in October 2022, Plaintiff again sought psychotherapy and mental health  
19 counseling services from Defendant, paying an additional \$965 for monthly subscriptions and add-  
20 on live therapy sessions.  
21

22           60. Plaintiff reasonably expected that her communications with Defendant via the  
23 Website and app were confidential, solely between herself and Defendant and her therapists, and  
24 that such communications would not be disclosed to a third party.

25           61. Plaintiff has an active Facebook account that she accesses on her computer and  
26 smartphone. She also has an active Pinterest account.  
27  
28

62. On information and belief and based on Defendant's standard practices as described herein and in the FTC complaint, Defendant disclosed Plaintiff's Private Information and communications to third parties, including when she completed her intake questionnaire on Defendant's Website.

63. On information and belief, information disclosed by Defendant to Facebook included Plaintiff's Facebook ID and allowed Facebook to link her Private Information to her Facebook account, allowing Facebook to target ads to Plaintiff.

64. Through the process detailed in this Complaint, Defendant disclosed Plaintiff's communications and Private Information, including those that contained personally identifiable information, protected health information, and related confidential information, to third parties. Defendant never disclosed to Plaintiff that it would disclose, sell, or otherwise share her Private Information with third parties. Instead, Defendant disclosed Plaintiff's Private Information without Plaintiff's knowledge, consent, or express written authorization.

65. Thus, Defendant misrepresented the manner in which it handled Plaintiff's Private Information and unlawfully disclosed Plaintiff's Private Information.

### CLASS ACTION ALLEGATIONS

66. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

67. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

**All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through a BetterHelp Website or App (including betterhelp.com, teencounseling.com, faithfulcounseling.com, pridecounseling.com, and regain.us).**

68. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any

1 successor or assign, and any Judge who adjudicates this case, including their staff and immediate  
2 family.

3 69. Plaintiff reserves the right to modify or amend the definition of the proposed classes  
4 before the Court determines whether certification is appropriate.

5 70. Numerosity, Fed R. Civ. P. 23(a)(1). The Class Members for each proposed Class  
6 are so numerous that joinder of all members is impracticable. Upon information and belief, there  
7 are millions of individuals whose Private Information may have been improperly disclosed to third  
8 parties, and the Class is identifiable within Defendant's records.

9 71. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common  
10 to each Class exist and predominate over any questions affecting only individual Class Members.  
11 These include:  
12

- 13 a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff  
14 and Class Members;
- 15 b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiff and Class  
16 Members to unauthorized third parties;
- 17 c. Whether Defendant violated its Privacy Policies by disclosing the PII and PHI of  
18 Plaintiff and Class Members to Facebook, Snapchat, Pinterest, Criteo, and/or  
19 additional third parties;
- 20 d. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class  
21 Members that their PII and PHI would be disclosed to third parties;
- 22 e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class  
23 Members that their PII and PHI had been compromised;
- 24 f. Whether Defendant adequately addressed and fixed the practices which permitted the  
25 disclosure of patient PHI and PII;
- 26  
27  
28

- g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;
- h. Whether Defendant violated the consumer protection statutes invoked herein;
- i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- j. Whether Defendant knowingly made false representations as to its data security and/or Privacy Policies practices;
- k. Whether Defendant knowingly omitted material representations with respect to its data security and/or Privacy Policies practices; and

72. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because each had their Private Information misused and disclosed as a result of Defendant's conduct.

73. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

74. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence,

1 effort, and expense that hundreds of individual actions would require. Class action treatment will  
2 permit the adjudication of relatively modest claims by certain Class Members, who could not  
3 individually afford to litigate a complex claim against large corporations, like Defendant. Further,  
4 even for those Class Members who could afford to litigate such a claim, it would still be  
5 economically impractical and impose a burden on the courts.

6  
7 75. Policies Generally Applicable to the Class. This class action is also appropriate for  
8 certification because Defendant has acted or refused to act on grounds generally applicable to the  
9 Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of  
10 conduct toward the Class Members and making final injunctive relief appropriate with respect to  
11 the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members  
12 uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to  
13 the Class as a whole, not on facts or law applicable only to Plaintiff.

14  
15 76. The nature of this action and the nature of laws available to Plaintiff and Class  
16 Members make the use of the class action device a particularly efficient and appropriate procedure  
17 to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would  
18 necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm  
19 the limited resources of each individual Class Member with superior financial and legal resources;  
20 the costs of individual suits could unreasonably consume the amounts that would be recovered;  
21 proof of a common course of conduct to which Plaintiff was exposed is representative of that  
22 experienced by the Class and will establish the right of each Class Member to recover on the cause  
23 of action alleged; and individual actions would create a risk of inconsistent results and would be  
24 unnecessary and duplicative of this litigation.

25  
26 77. The litigation of the claims brought herein is manageable. Defendant's uniform  
27 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class  
28

1 Members demonstrate that there would be no significant manageability problems with prosecuting  
2 this lawsuit as a class action.

3 78. Adequate notice can be given to Class Members directly using information  
4 maintained in Defendant's records.

5 79. Unless a Class-wide injunction is issued, Defendant may continue in its failure to  
6 properly secure the Private Information of Class Members, Defendant may continue to refuse to  
7 provide proper notification to Class Members regarding the practices complained of herein, and  
8 Defendant may continue to act unlawfully as set forth in this Complaint.

9 80. Further, Defendant has acted or refused to act on grounds generally applicable to  
10 each Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the  
11 Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil  
12 Procedure.

13 81. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification  
14 because such claims present only particular, common issues, the resolution of which would advance  
15 the disposition of this matter and the parties' interests therein. Such particular issues include, but  
16 are not limited to:

- 17 a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members'  
18 Private Information;  
19 b. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members'  
20 Private Information with respect to Defendant's Privacy Policies;  
21 c. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise  
22 due care in collecting, storing, using, and safeguarding their Private Information;  
23 d. Whether Defendant failed to comply with its own policies and applicable laws,  
24 regulations, and industry standards relating to data security;  
25  
26  
27  
28

- 1 e. Whether Defendant adequately and accurately informed Plaintiff and Class Members  
2 that their Private Information would be disclosed to third parties;  
3  
4 f. Whether Defendant failed to implement and maintain reasonable security procedures  
5 and practices appropriate to the nature and scope of the information disclosed to third  
6 parties; and  
7  
8 g. Whether Class Members are entitled to actual, consequential, and/or nominal  
9 damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

10 82. Plaintiff reserves the right to amend or modify the Class definition as this case  
11 progresses.

12 **COUNT I**  
13 **BREACH OF IMPLIED CONTRACT**  
14 **(On behalf of Plaintiff and the Nationwide Class)**

15 83. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint  
16 as if fully set forth herein.

17 84. When Plaintiff and Class Members provided their Private Information to Defendant  
18 in exchange for services, they entered into an implied contract pursuant to which Defendant agreed  
19 to safeguard and not disclose their Private Information without consent.

20 85. Plaintiff and Class Members accepted Defendant's offers and provided their Private  
21 Information to Defendant.

22 86. Plaintiff and Class Members would not have entrusted Defendant with their Private  
23 Information in the absence of an implied contract between them and Defendant obligating Defendant  
24 to not disclose Private Information without consent.

25 87. Defendant breached these implied contracts by disclosing Plaintiff's and Class  
26 Members' Private Information to third parties, including Facebook, Snapchat, Pinterest, and Criteo.

27 88. As a direct and proximate result of Defendant's breaches of these implied contracts,  
28 Plaintiff and Class Members sustained damages as alleged herein. Plaintiff and Class Members

1 would not have used Defendant's services, or would have paid substantially for these services, had  
 2 they known their Private Information would be disclosed.

3 89. Plaintiff and Class Members are entitled to compensatory and consequential damages  
 4 as a result of Defendant's breach of implied contract.

5  
 6 **COUNT II**  
**VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW**  
**Cal. Bus. & Prof. Code § 17200**  
 7

8 90. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set  
 9 forth herein and brings this claim individually and on behalf of the proposed Class.

10 91. This Count is pleaded in the alternative to the breach of contract count above.

11 92. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or  
 12 fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal.  
 13 Bus. & Prof. Code § 17200.  
 14

15 93. Defendant engaged in unlawful business practices in connection with its disclosure  
 16 of Plaintiff's and Class Members' Private Information to unrelated third parties, including  
 17 Facebook, Snapchat, Pinterest, and Criteo, in violation of the UCL.

18 94. The acts, omissions, and conduct of Defendant were controlled, directed, and  
 19 emanated from its California headquarters.  
 20

21 95. The acts, omissions, and conduct of Defendant as alleged herein constitute "business  
 22 practices" within the meaning of the UCL.

23 96. Defendant violated the "unlawful" prong of the UCL by violating, inter alia,  
 24 Plaintiff's and Class Member's constitutional rights to privacy, state and federal privacy statutes,  
 25 and state consumer protection statutes, such as HIPAA and the California Confidentiality of  
 26 Information Act ("CMIA"). Defendant also violated the unlawful prong of the UCL by  
 27  
 28

1 disseminating false and misleading statements regarding its privacy practices in violation of  
2 California's False Advertising Laws.

3       97. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL  
4 because those acts, omissions, and conduct, as alleged herein, offended public policy (including the  
5 aforementioned federal and state privacy statutes and state consumer protection statutes, such as  
6 HIPAA and CMIA and constitute immoral, unethical, oppressive, and unscrupulous activities that  
7 caused substantial injury, including to Plaintiff and Class Members.

8       98. Defendant's acts, omissions, and conduct also violate the fraudulent prong of the  
9 UCL because Defendant made material misrepresentations and omissions of fact to induce Plaintiff  
10 and Class Members to purchase Defendant's services without disclosing that Defendant shared,  
11 used, and sold Plaintiff's and Class Members Private Information and without obtaining consent.  
12 Defendant's acts, omissions, nondisclosures, and misleading statements as alleged herein were and  
13 are false, misleading, and/or likely to deceive the consuming public.  
14

15       99. Plaintiff viewed and relied upon Defendant's representations concerning the  
16 confidentiality of information provided by Plaintiff and Class Members to Defendant. Had  
17 Defendant disclosed that it shared Private Information with third parties, Plaintiff would not have  
18 purchased Defendant's services or would have paid considerably less for those services.  
19

20       100. The harm caused by the Defendant's conduct outweighs any potential benefits  
21 attributable to such conduct and there were reasonably available alternatives to further Defendant's  
22 legitimate business interests other than Defendant's conduct described herein.  
23

24       101. As result of Defendant's violations of the UCL, Plaintiff and Class Members have  
25 suffered injury in fact and lost money or property, including but not limited to payments to  
26 Defendant and/or other valuable consideration, *e.g.*, access to their private and personal data. The  
27  
28

1 unauthorized access to Plaintiff's and Class Members' private and personal data also has diminished  
2 the value of that information.

3  
4 **COUNT III**  
5 **VIOLATION OF CALIFORNIA FALSE ADVERTISING LAW**  
6 **Cal. Bus. & Prof. Code § 17500**

7 102. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set  
8 forth herein and brings this claim individually and on behalf of the proposed Class.

9 103. This Count is pleaded in the alternative to the breach of contract count above.

10 104. The acts, omissions, and conduct of Defendant were controlled, directed, and  
11 emanated from its California headquarters.

12 105. California's False Advertising Law, Cal. Bus. & Prof. Code § 17500, et seq., makes  
13 it "unlawful for any person to make or disseminate or cause to be made or disseminated before the  
14 public in this state, ... in any advertising device ... or in any other manner or means whatever,  
15 including over the Internet, any statement, concerning ... personal property or services, professional  
16 or otherwise, or performance or disposition thereof, which is untrue or misleading and which is  
17 known, or which by the exercise of reasonable care should be known, to be untrue or misleading.

18 106. Defendant committed acts of false advertising, as defined by § 17500, by  
19 intentionally making and disseminating statements to consumers in California and the general public  
20 concerning Defendant's products and services, as well as circumstances and facts connected to such  
21 products and services, which are untrue and misleading on their face and by omission, and which  
22 are known (or which by the exercise of reasonable care should be known) by Defendant to be untrue  
23 or misleading. Defendant has also intentionally made or disseminated such untrue or misleading  
24 statements and material omissions to consumers in California and to the public as part of a plan or  
25 scheme with intent not to sell those services as advertised.  
26  
27  
28

1           107. Defendant's statements include but are not limited to representations and omissions  
2 made to consumers in the intake questionnaire and privacy policy regarding Defendant's  
3 commitment to maintain the privacy of Private Information and not to disclose Private Information  
4 to third parties. Such representations and omissions constitute false and deceptive advertisements.

5           108. Plaintiff viewed and relied upon Defendant's representations concerning the  
6 confidentiality of information provided by Plaintiff and Class Members to Defendant. Had  
7 Defendant disclosed that it shared Private Information with third parties, Plaintiff would not have  
8 purchased Defendant's services or would have paid considerably less for those services.

9           109. Defendant's actions in violation of § 17500, as described herein, were false and  
10 misleading such that the general public is and was likely to be deceived. Plaintiff and the members  
11 of the Class were deceived by Defendant's statements and omissions made online when they signed  
12 up and started paying for BetterHelp services, and there is a strong probability that consumers and  
13 members of the public were also or are likely to be deceived as well. Any reasonable consumer  
14 would be misled by Defendant's false and misleading statements and material omissions. Plaintiff  
15 and other members of the Class did not learn of Defendant's disclosure of their Private Information  
16 until after they had already signed up and paid for Defendant's services and the FTC settlement was  
17 announced. They relied on Defendant's statements and omissions to their detriment.

18           110. Plaintiff and the Class lost money or property as a result of Defendant's FAL  
19 violations because they would not have purchased BetterHelp services on the same terms if the true  
20 facts were known about the product and the BetterHelp services do not have the characteristics as  
21 promised by Defendant. Plaintiff, individually and on behalf of all similarly situated consumers,  
22 seeks individual, representative, and public injunctive relief and any other necessary orders or  
23 judgments that will prevent Defendant from continuing with its false and deceptive advertisements  
24  
25  
26  
27  
28

1 and omissions; restitution that will restore the full amount of their money or property; disgorgement  
2 of Defendant's relevant profits and proceeds; and an award of costs and reasonable attorneys' fees.

3  
4 **COUNT IV - VIOLATION OF THE CALIFORNIA**  
**CONFIDENTIALITY OF MEDICAL INFORMATION ACT**

5 **Cal. Civ. Code § 56, *et seq***

6 111. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully  
7 set forth herein and brings this claim individually and on behalf of the proposed Class.

8 112. The California Confidentiality of Medical Information Act, Cal. Civ. Code § 56,  
9 *et seq* ("CMIA") prohibits health care providers from disclosing medical information relating to  
10 their patients without a patient's authorization. "Medical information" refers to "any individually  
11 identifiable information, in electronic or physical form, in possession of or derived from a  
12 provider of health care... regarding a patient's medical history, mental or physical condition, or  
13 treatment. 'Individually Identifiable' means that the medical information includes or contains any  
14 element of personal identifying information sufficient to allow identification of the individual..."  
15 Cal. Civ. Code § 56.05.

16  
17 113. Defendant is a healthcare provider as defined by Cal. Civ. Code § 56.06.

18 114. Plaintiff and Class Members are patients, and, as a health care provider, Defendant  
19 has an ongoing obligation to comply with the CMIA's requirements.

20 115. As set forth above, names, addresses, telephone numbers, email addresses, device  
21 identifiers, web URLs, Internet Protocol (IP) addresses, and other characteristics that can  
22 uniquely identify Plaintiff and Class members are transmitted to in combination with patient  
23 mental health concerns, treatment(s) sought, medications, and whether the patient is suffering  
24 from anxiety, depression, or a number of other mental health symptoms. This protected health  
25 information and personally identifiable information constitutes confidential information under  
26 the CMIA. This information is collected, recorded, and stored by Defendant and intentionally  
27 disclosed to third parties without Plaintiff's and Class Members' knowledge or consent.  
28

1           116. Facebook ID is also an identifier sufficient to allow identification of an individual.  
2           Along with patients' confidential Private Information, Defendant discloses to Facebook the  
3           patient's FID.

4           117. Pursuant to the CMIA, the information communicated to Defendant and disclosed  
5           to third parties constitutes medical information because it is patient information derived from a  
6           health care provider regarding patients' medical treatment and physical and mental condition and  
7           is in combination with individually identifying information. Cal. Civ. Code § 56.05(i).

8           118. As set forth above, Facebook and other third parties view, process, and analyze  
9           the confidential medical information it receives from Defendant and uses that Private Information  
10          for advertising and marketing purposes.

11          119. As demonstrated hereinabove, Defendant fails to obtain its patients' authorization  
12          for the disclosure of medical information and fails to disclose in its Website Privacy Policy that  
13          it shares protected health information with third parties for their marketing purposes.

14          120. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical  
15          information must be: (1) "Clearly separate from any other language present on the same page and  
16          is executed by a signature which serves no other purpose than to execute the authorization;" (2)  
17          signed and dated by the patient or her representative; (3) state the name and function of the third  
18          party that receives the information; (4) state a specific date after which the authorization expires.  
19          Accordingly, the information set forth in Defendant's Website Privacy Policy and any Terms and  
20          Conditions do not qualify as a valid authorization.

21          121. Based on the above, Defendant is violating the CMIA by disclosing its patients'  
22          medical information to third parties along with the patients' individually identifying information.  
23          Accordingly, Plaintiff and Class Members seek all relief available for Defendant's CMIA  
24          violations.  
25  
26  
27  
28

1 122. Plaintiff and members of the Class seek nominal damages, compensatory  
2 damages, punitive damages, attorneys' fees and costs of litigation for Defendant's violation of  
3 the CMIA.

4 **COUNT IV**  
5 **UNJUST ENRICHMENT**  
6 **(On behalf of Plaintiff and the Nationwide Class)**

7 123. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint  
8 as if fully set forth herein.

9 124. This Count is pleaded in the alternative to the breach of contract count above.

10 125. Defendant benefits from the use of Plaintiff's and Class Members' Private  
11 Information and unjustly retained those benefits at their expense.

12 126. Plaintiff and Class Members conferred a benefit upon Defendant in the form of  
13 Private Information that Defendant collected from Plaintiff and Class Members, without  
14 authorization and proper compensation. Defendant consciously collected and used this information  
15 for its own gain, providing Defendant with economic, intangible, and other benefits, including  
16 substantial monetary compensation.

17 127. Defendant unjustly retained those benefits at the expense of Plaintiff and Class  
18 Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing  
19 any commensurate compensation to Plaintiff and Class Members.

20 128. The benefits that Defendant derived from Plaintiff and Class Members was not  
21 offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class  
22 Members. It would be inequitable under unjust enrichment principles in Missouri and every other  
23 state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from  
24 the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.  
25  
26  
27  
28

129. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

### RELIEF REQUESTED

130. Plaintiff, on behalf of herself and the proposed Class, respectfully requests that the Court grant the following relief:

(a) Certification of this action as a class action pursuant to Federal Rule of Civil Procedure 23 and appointment of Plaintiff and Plaintiff's counsel to represent the Class;

(b) An order enjoining Defendant from engaging in the unlawful practices and illegal acts described herein;

(c) An order awarding Plaintiff and the Class: (1) actual or statutory damages; (2) punitive damages—as warranted—in an amount to be determined at trial; (3) prejudgment interest on all amounts awarded; (4) injunctive relief as the Court may deem proper; (5) reasonable attorneys' fees and expenses and costs of suit pursuant to applicable law; and (6) such other and further relief as the Court may deem appropriate.

### DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the proposed Class, demand a trial by jury for all of the claims asserted in this Complaint so triable.

Dated: March 7, 2023

Respectfully submitted,

By: 

John J. Nelson (SBN 317598)  
**MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN, PLLC**  
401 W. Broadway, Suite 1760  
San Diego, CA 92101  
Telephone: (858) 209-6941  
Fax: (865) 522-0049  
Email: [jnelson@milberg.com](mailto:jnelson@milberg.com)

1 Gary M. Klinger\*  
2 Glen L. Abramson\*  
3 Alexandra M. Honeycutt\*  
4 **MILBERG COLEMAN BRYSON**  
5 **PHILLIPS GROSSMAN, PLLC**  
6 227 W. Monroe Street, Suite 2100  
7 Chicago, Illinois 60606  
8 Telephone: 866.252.0878  
9 [gklinger@milberg.com](mailto:gklinger@milberg.com)  
10 [gabramson@milberg.com](mailto:gabramson@milberg.com)  
11 [ahoneycutt@milberg.com](mailto:ahoneycutt@milberg.com)

12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  

*\*Pro Hac Vice Application Forthcoming*

*Attorneys for Plaintiff and the Putative Class*

# EXHIBIT A

2023169

**UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:**      **Lina M. Khan, Chair**  
                                 **Rebecca Kelly Slaughter**  
                                 **Christine S. Wilson**  
                                 **Alvaro M. Bedoya**

**In the Matter of**

**BETTERHELP, INC., a corporation,  
also d/b/a  
COMPILE, INC.,  
also d/b/a MYTHERAPIST,  
also d/b/a TEEN COUNSELING,  
also d/b/a FAITHFUL COUNSELING,  
also d/b/a PRIDE COUNSELING,  
also d/b/a ICOUNSELING,  
also d/b/a REGAIN,  
also d/b/a TERAPPEUTA.**

**DOCKET NO.**

**COMPLAINT**

The Federal Trade Commission (“FTC” or “Commission”), having reason to believe that BetterHelp, Inc., a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent BetterHelp, Inc. (“BetterHelp” or “Respondent”), 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 at 990 Villa Street, Mountain View, CA 94041.
2. Respondent has developed, advertised, and offered for sale an online counseling service (the “Service”)—including specialized versions of the Service for people of the Christian faith, members of the LGBTQ community, and teenagers—which matches users with Respondent’s therapists and then facilitates counseling via Respondent’s websites and apps.
3. Millions of consumers have signed up for the Service, entrusting Respondent with their email addresses, IP addresses, and certain information about their health status and histories—such as the fact that they are seeking or are in therapy, and whether they have previously been in therapy. Because Respondent collects certain types of personal information from consumers when they take affirmative steps to sign up for the Service, Respondent’s disclosure of that information to a third party would implicitly disclose the consumer’s interest in or use of the

Service and therefore constitute a disclosure of the consumer's health information. For example, because Respondent obtained a consumer's email address only when the consumer took affirmative steps to utilize the Service, Respondent's disclosure of this information would identify the consumer as associated with seeking and/or receiving mental health treatment. Similarly, Respondent's disclosure that a consumer took affirmative steps to sign up for the Service (such as by filling out Respondent's intake questionnaire for the Service or becoming a paying user), along with an identifier (for example, an IP address), would disclose the consumer's seeking of mental health treatment via the Service.

4. Recognizing the sensitivity of this health information, Respondent has repeatedly promised to keep it private and use it only for non-advertising purposes such as to facilitate consumers' therapy.

5. From 2013 to December 2020, however, Respondent continually broke these privacy promises, monetizing consumers' health information to target them and others with advertisements for the Service. For example, from 2018 to 2020, Respondent used these consumers' email addresses and the fact that they had previously been in therapy to instruct Facebook to identify similar consumers and target them with advertisements for the Service, bringing in tens of thousands of new paying users, and millions of dollars in revenue, as a result.

6. To capitalize on these consumers' health information, Respondent handed it over to numerous third-party advertising platforms, including Facebook, Pinterest, Snapchat, and Criteo, often permitting these companies to use the information for their own research and product development as well.

7. In addition, Respondent failed to employ reasonable measures to safeguard the health information it collected from consumers. In particular, Respondent did not properly train its employees on how to protect the information when using it for advertising, and Respondent did not properly supervise its staff in the use of the information. Respondent also failed to provide consumers with proper notice as to the collection, use, and disclosure of their health information. And Respondent failed to limit contractually how third parties could use consumers' health information, instead merely agreeing to their stock contracts and terms.

8. It was only in December 2020, well after reporters brought these practices to light and the FTC began investigating the practices, that Respondent curtailed its unauthorized use and disclosure of consumers' health information.

9. The acts and practices of Respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

## **I. Background**

### **A. The Service**

10. Respondent offers the Service under several names, each of which has its own website and app (collectively, the "Multi-Sites"). Its primary website and app, which is named "BetterHelp," serves general audiences and has been in operation since 2013. Faithful Counseling, in operation since July 2017, is aimed at consumers of the Christian faith. Pride

Counseling, in operation since August 2017, caters to the LGBTQ community. Teen Counseling, in operation since January 2017, offers counseling to 13- to 18-year-olds with parental consent. And ReGain, in operation since May 2016, offers couples counseling.<sup>1</sup> The Multi-Sites all function similarly and facilitate therapy via the Service, and they are all subject to Respondent's policies, practices, and procedures.

11. Users pay \$60 to \$90 per week for counseling through the Service. To sign up for the Service and become a paying user (a "User"), an individual visiting one of the Multi-Sites (a "Visitor") must fill out a questionnaire (the "Intake Questionnaire"), answering detailed questions about the Visitor's mental health.

12. Upon completing the Intake Questionnaire, a Visitor is prompted to create an account for the Service by entering the Visitor's name or nickname, email address, phone number, and emergency contact information. The Visitor is then asked to enter credit card information to become a paying User.

13. Respondent then utilizes the User's responses to the Intake Questionnaire to match the User with one of Respondent's more than 25,000 licensed therapists. Respondent's therapists provide Users with mental health therapy via video conferencing, text messaging, live chat, and audio calls.

14. Respondent's primary website and app, "BetterHelp," has seen explosive growth over the last few years, 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, and, today, it has over 374,000 active Users in the United States. As a result, Respondent earned over \$345 million in revenue in 2020, and over \$720 million in revenue in 2021.

## **B. Respondent's Marketing History**

15. Since its inception, Respondent has utilized numerous third parties to market the Service, including, at various times, Facebook, Snapchat, Pinterest, and Criteo. In addition, Respondent has advertised the Service on search engines, television, podcasts, and radio.

16. In 2017, Respondent delegated most decision-making authority over its use of Facebook's advertising services to a Junior Marketing Analyst who was a recent college graduate, had never worked in marketing, and had no experience and little training in safeguarding consumers' health information when using that information for advertising. In doing so, Respondent gave the Junior Marketing Analyst carte blanche to decide which Visitors' and Users' health information to upload to Facebook and how to use that information. This same individual, who now holds the title "Senior Marketing Analyst," continues to oversee Respondent's use of Facebook's advertising tools.

17. Respondent provided this marketing analyst with little training on how to protect Visitors' and Users' health information in connection with advertising until 2021. In fact, while

---

<sup>1</sup> Respondent also offered the Service through the iCounseling website and app from February 2017-November 2020, the Terapeuta website and app from March 2017-March 2019, and the MyTherapist website and app from June 2017-March 2019.

Respondent has purported to provide privacy training to its employees since 2015, it was not until 2021 that Respondent gave them any training specific to its business or advertising.

18. Respondent has spent tens of millions of dollars annually to market the Service. In 2020, for example, it spent \$10-\$20 million on Facebook advertising, and by 2021 Respondent's advertising on Facebook was bringing in approximately 30,000 to 40,000 new Users per quarter.

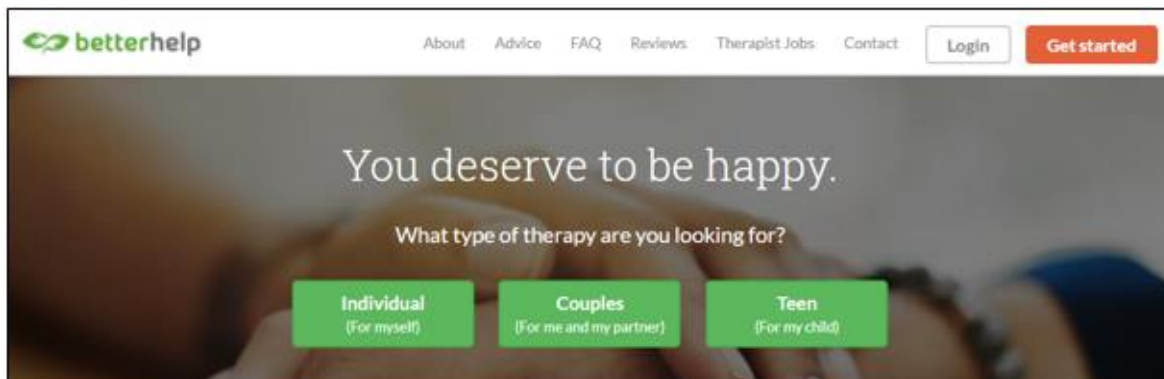
## **II. Respondent's Deceptive Business Practices**

19. In connection with the advertisement and sale of the Service, Respondent has disseminated, or caused to be disseminated, false and deceptive statements about its use and disclosure of consumers' health information. Respondent also disseminated, or caused to be disseminated, misleading and deceptive representations regarding its compliance with federal health privacy laws. Visitors and Users relied on these representations and were misled as a result.

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

#### Respondent's deceptive statements concerning Intake Questionnaire responses

20. Upon arriving at any of the Multi-Sites, a Visitor is immediately prompted to begin the 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:



21. After making a selection, the Visitor is ushered through the Intake Questionnaire, which asks an array of questions. For many Visitors, these questions include whether the Visitor is "experiencing overwhelming sadness, grief, or depression"; whether the Visitor has been having thoughts that the Visitor "would be better off dead or hurting yourself in some way"; whether the Visitor is "currently taking any medication"; whether the Visitor has "problems or worries about intimacy"; and whether the Visitor has previously been in therapy.

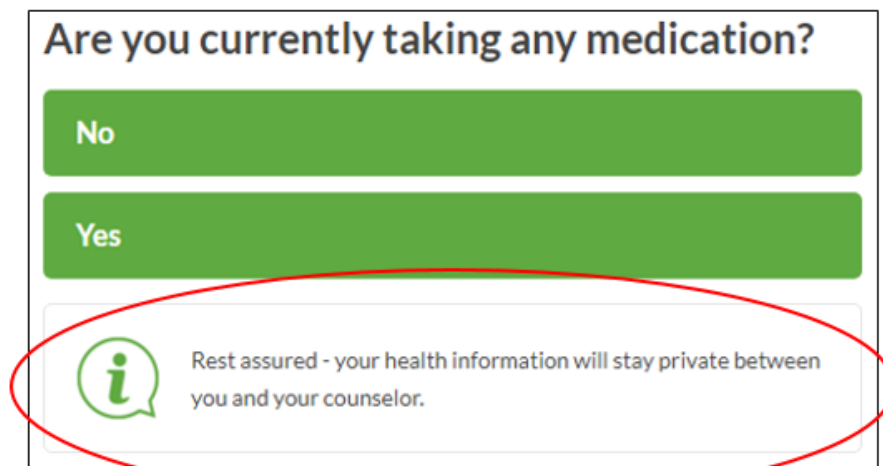
22. The Intake Questionnaire also asks whether the Visitor identifies as a member of the Christian faith, shuttling such individuals to Faithful Counseling. Similarly, the Intake Questionnaire takes those who identify as members of the LGBTQ community to Pride

Counseling. And Respondent ushers teenagers to Teen Counseling, where the teenage Visitors provide their responses to the Intake Questionnaire before Respondent obtains parental consent.

23. Respondent has included privacy assurances throughout the Intake Questionnaire. Until November 2021, each Multi-Site displayed a banner at the top of each question, explaining that Respondent 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 Visitor can be matched “with the most suitable therapist for you.”

24. As Visitors proceed through the Intake Questionnaire, Respondent includes additional periodic privacy assurances. From at least August 2017 to December 2020, when a Visitor reached the question as to whether the Visitor was taking medication, the Visitor was shown the statement: “Rest assured—any information provided in this questionnaire will stay private between you and your counselor.”


25. In December 2020, Respondent changed the statement to read: “Rest assured—*this information* will stay private between you and your counselor” (emphasis on alteration added). And in January 2021, Respondent changed it again to state: “Rest assured—*your health information* will stay private between you and your counselor” (emphasis on alteration added). This version, which was in use until September 2021, is circled in red below:



Are you currently taking any medication?

No

Yes

 Rest assured - your health information will stay private between you and your counselor.

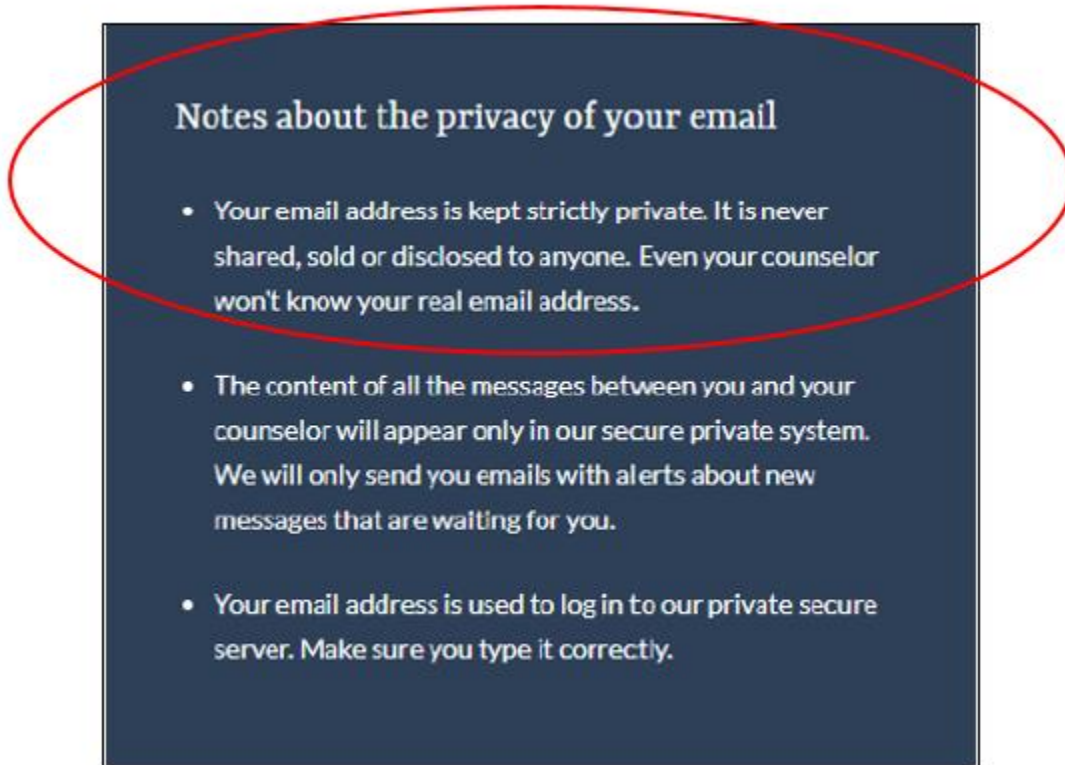
In October 2021, Respondent removed this representation altogether.

26. After being presented with these repeated promises of privacy, millions of Visitors, including those that became Users, filled out the Intake Questionnaire and shared their health information with Respondent.

27. Despite the aforementioned assurances of privacy, Respondent disclosed Visitors’ and 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 discussed in Paragraphs 51-54 and 57 below.

Respondent falsely promised to keep Christian, LGBTQ, and teenage consumers' email addresses "strictly private"

28. From at least August 2017 to as recently as December 2020, Respondent gave additional privacy assurances to Faithful Counseling, Pride Counseling, and Teen Counseling Visitors to induce them to sign up for the Service, stating that their email addresses would be "kept strictly private" and "never shared, sold or disclosed to anyone." This representation, which Respondent displayed prominently and unavoidably during the sign-up process, is circled in red below:



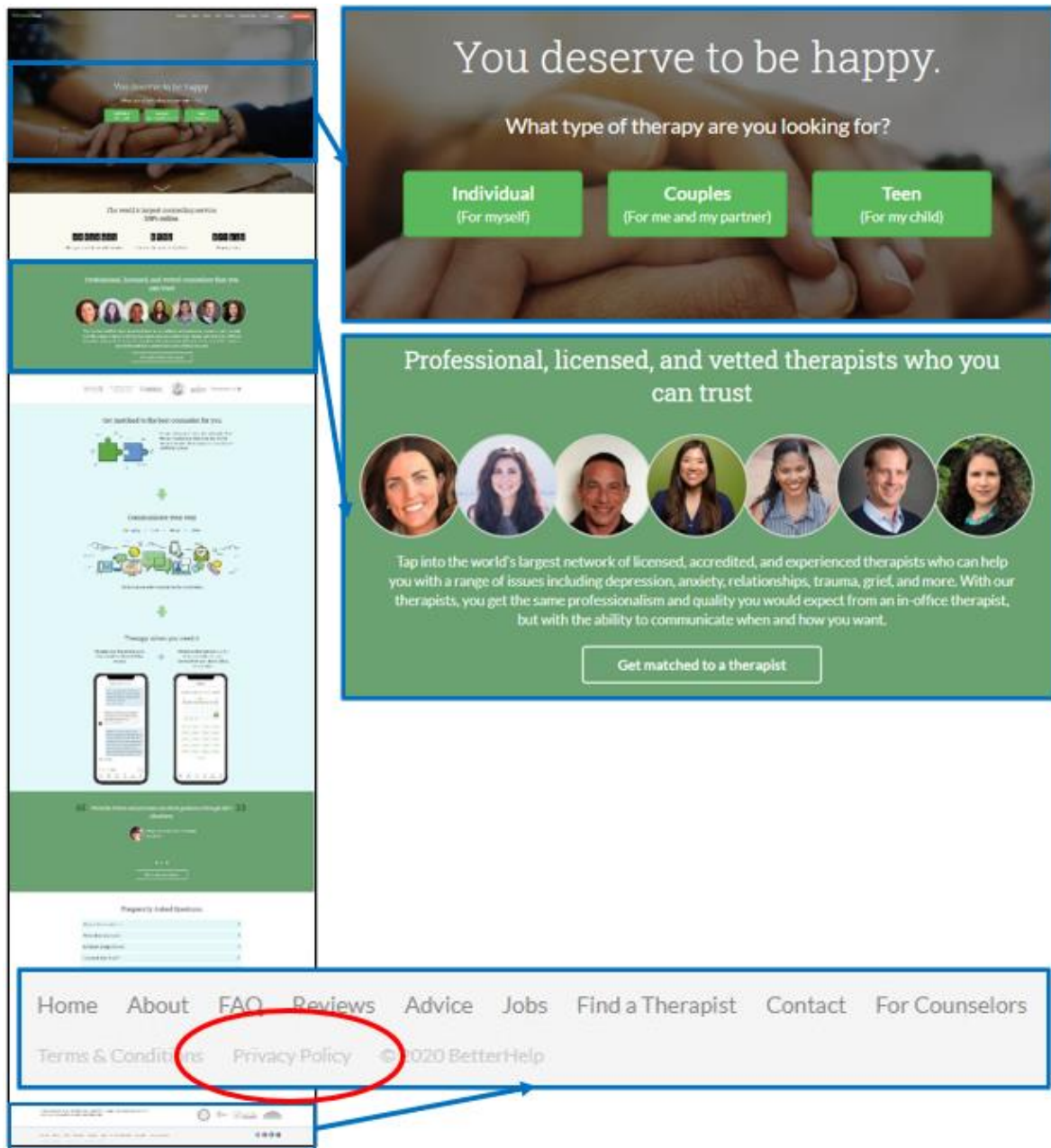
29. Tens of thousands of Visitors provided Respondent with their email addresses and signed up for Faithful Counseling, Pride Counseling, and Teen Counseling after viewing this privacy assurance.

30. Respondent understood that its disclosure of Visitors' email addresses in association with BetterHelp would reveal that the Visitors were seeking mental health treatment through the Service. And Respondent understood that consumers would want to keep this information private. In fact, a senior BetterHelp employee acknowledged at an investigational hearing conducted by FTC staff that individuals "want to keep . . . the fact that they're in therapy private" and at times even "keep their identities . . . secret from their therapist[s]."

31. Nevertheless, Respondent disclosed the email addresses of thousands of these Visitors to various third parties for advertising purposes and the third parties' own purposes, as discussed in further detail in Paragraphs 47-55 and 57, thereby revealing to the third parties that these Visitors were seeking and/or receiving mental health treatment via the Service.

Respondent pushed Visitors and Users into disclosing their health information

32. In addition to making false representations, Respondent has pushed Visitors and Users into handing over their health information before they have ever had a chance to read any privacy disclosures.
33. Upon visiting any of the Multi-Sites, Visitors are urged to begin the Intake Questionnaire and hand over their health information. At the same time, Visitors are repeatedly presented with the aforementioned privacy assurances discussed in Paragraphs 23-25 and 28—displayed in large, high-contrast, unavoidable text.
34. By contrast, Respondent linked to the privacy policy in small, low-contrast writing that is barely visible at the bottom of the page.
35. The image below depicts the BetterHelp homepage ([www.betterhelp.com](http://www.betterhelp.com)), with the prompts to enter the Intake Questionnaire magnified at the top and the link to the privacy policy magnified at the bottom and circled in red:



36. In September 2020, Respondent added the below banner to the bottom of every page of its Multi-Sites (until a Visitor closed it), which stated: “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.”



37. Despite including a link to the privacy policy, the banner effectively dissuaded Visitors from reading the privacy policy by stating, until October 2020, that Respondent would “never sell or rent any information you share with us.”

38. In May 2021, Respondent revised the banner and added 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). But this banner still did not inform Visitors that Respondent would use and disclose their health information for advertising or that third parties would be able to use Visitors’ information for their own purposes.

39. It was not until October 2021 that Respondent revised the banner to state that it discloses Visitors’ IP addresses and other personal identifiers for advertising and offered Visitors an opportunity to opt out of the disclosures via the banner.

Respondent’s privacy policies claimed limited use and disclosure of consumers’ information

40. Those Visitors and Users that persevered and read Respondent’s privacy policy were presented with additional deceptive statements about Respondent’s use and disclosure of health information.

41. From August 2013 to November 2018, Respondent’s privacy policies represented that it would use and disclose Visitors’ and Users’ 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. Notably, these privacy policies made no mention of using or disclosing this information for advertising purposes, and they said nothing about permitting third parties to use this information for their own purposes.

42. In November 2018, Respondent 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. These limited purposes did not include using or disclosing the information for advertising or disclosing the information to third parties for their own purposes.

43. Respondent revised its privacy policy again in September 2019, stating that it might *use* this health information for advertising. But the policy continued to say that Respondent 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, Respondent revised the privacy policy yet again, finally stating that it may *both use and disclose* Visitors’ and Users’ information for advertising. But, even then, the privacy policy continued to claim that Respondent would disclose this information to third parties for only the stated limited purposes, which did not include third parties’ own purposes.

44. 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 Visitors’ or Users’ health information for advertising purposes, or the disclosure of this information for third parties’ own purposes. These tools allow

Respondent and third parties to collect Visitors' and Users' information when they use one of the Multi-Sites, including what pages a Visitor or User visits and what information a Visitor or User inputs into the website (which would include the Visitor's or User's email address, IP address, and certain Intake Questionnaire responses).

45. But, as discussed in Paragraphs 46-57 below, these privacy policy representations misled Visitors and Users. In fact, Respondent used and disclosed Visitors' and Users' health information for advertising purposes, and Respondent disclosed this information to third parties for their own purposes, from 2013 to December 2020. Respondent used and disclosed this information for advertising purposes through various means, including by uploading consumers' email addresses to third-party advertising platforms and through web beacons (specifically pixels) Respondent had placed on various pages of the Multi-Sites.

### **B. Respondent Used and Disclosed Millions of Consumers' Health Information for Advertising**

46. Since 2013, Respondent has repeatedly broken each of its aforementioned privacy promises, using Visitors' and Users' email addresses, IP addresses, enrollment in the Service, and certain Intake Questionnaire responses for various advertising purposes, including (1) re-targeting Visitors with advertisements for the Service; (2) using Users' health information to find and target potential new Users with advertisements—on the basis that these potential new Users were likely to sign up for the Service because they shared traits with current Users; and (3) optimizing Respondent's advertisements, which involved targeting advertisements at individuals with attributes similar to those that had previously responded to Respondent's ads, such as new Users. Using this health information for advertising, Respondent has brought in hundreds of thousands of new Users, resulting in millions of dollars in additional revenue.

47. Respondent utilized a number of third-party advertising platforms, including Facebook, Snapchat, Criteo, and Pinterest, to carry out this advertising. To do so, Respondent disclosed Visitors' and Users' email addresses, IP addresses, enrollment in the Service, and certain Intake Questionnaire responses to these third parties, as detailed below.

48. As noted above, each such disclosure of even a Visitor's or User's email address constituted a disclosure of the Visitor's or User's health information. Specifically, because Respondent collected email addresses only from Visitors and Users 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 a Visitor's or User's email address implicitly identified the Visitor or User as one seeking and/or receiving mental health treatment via the Service.

49. Although Respondent "hashed" Visitors' and Users' email addresses (i.e., converted the email addresses into a sequence of letters and numbers through a cryptographic tool) before disclosing them to third parties, the hashing was not meant to conceal the Visitors' and Users' identities from Facebook or the other recipient third parties. Rather, the hashing was done merely to hide the email addresses from a bad actor in the event of a security breach. In fact, Respondent knew that third parties such as Facebook were able to, and in fact would, effectively undo the hashing and reveal the email addresses of those Visitors and Users with accounts on the respective third parties' platforms, which is how Facebook matched these email addresses with

Facebook user IDs. Indeed, Facebook's standard terms of service, to which Respondent agreed, explained that Facebook would use hashed email addresses it received from Respondent to match Visitors and Users with their Facebook user IDs for advertising purposes, among other things. Thus, Respondent knew that by sending these lists of Visitors' and Users' email addresses to third parties, it was telling these third parties which of their users were seeking or in therapy through the Service.

50. In addition, Respondent disclosed the Visitor's or User's IP address in conjunction with other data about their enrollment in the Service and/or their Intake Questionnaire responses to third parties. Each such disclosure similarly constituted a disclosure of the Visitor's or User's health information because it both identified the individual (via the IP address) and conveyed to the recipient third party that the Visitor or User was seeking and/or receiving mental health treatment via the Service (via his or her enrollment in the Service or answering the Intake Questionnaire).

51. **Health information shared with Facebook:** Respondent disclosed Visitors' and Users' health information to Facebook in two ways.

52. First, Respondent compiled lists of Visitors' and Users' email addresses, which it then uploaded to Facebook to match these individuals to their Facebook user accounts in order to target them and others like them with advertisements. Between 2017 and 2018, Respondent uploaded lists of over 7 million Visitors' and Users' email addresses to Facebook. Facebook matched over 4 million of these Visitors and Users with their Facebook user IDs, linking their use of the Service for mental health treatment with their Facebook accounts. Several examples are listed below:

- a. January 2017 – October 2018: Respondent uploaded over 170,000 Visitors' and Users' email addresses to Facebook, re-targeting these individuals and targeting potential new Users with advertisements for the Service.
- b. January 2018 – October 2018: Respondent uploaded over 15,000 Users' email addresses to Facebook to find and target new potential Users with advertisements for the Service.
- c. October 2017: Respondent uploaded 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.

53. Second, from 2013 to December 2020, Respondent shared Visitors' and Users' email addresses, IP addresses, and records known as "Events" with Facebook. These Events automatically tracked certain actions of each Visitor and User on the Multi-Sites, such as when they answered certain questions on the Intake Questionnaire in a certain way or when a Visitor enrolled in the Service to become a User. Respondent recorded and automatically disclosed these Events to Facebook through web beacons Respondent had placed on each of the Multi-Sites. Respondent disclosed Visitors' and Users' IP addresses, email addresses, and/or other persistent identifiers to Facebook alongside the Events so that Facebook could match the Events

information with the Visitors' and Users' Facebook accounts for advertising. Several examples are listed below:

- a. January 2018: Respondent disclosed to Facebook that over 70,000 Visitors 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: Respondent disclosed to Facebook over 1.5 million Visitors' and Users' previous therapy—gathered through their affirmative responses to the Intake Questionnaire question “Have you been in counseling or therapy before?”—to re-target the Visitors with advertisements and optimize Respondent's advertisements.
- c. October 2018 – November 2020: Respondent used and shared over 3.5 million Visitors' and Users' “good” or “fair” financial status—gathered through the Intake Questionnaire—with Facebook to optimize Respondent's advertisements and to find potential new Users and target them with advertisements.
- d. January – December 2020: Respondent shared with Facebook the fact that over 180,000 Visitors had become paying Users—through an Event denoting they had entered credit card information after completing the Intake Questionnaire—to optimize Respondent's advertisements and to find potential new Users and target them with advertisements.

54. Respondent labeled the Intake Questionnaire responses concerning prior therapy and financial status with anonymous Event titles before giving them to Facebook; however, in July 2018, the previously mentioned inexperienced and insufficiently trained Junior Marketing Analyst whom Respondent had put in charge of Facebook advertising revealed certain Events' true meaning to Facebook via the Facebook employee that serviced Respondent's advertising account. For example, though an affirmative response to the question “Have you been in counseling or therapy before?” was coded as “AddToWishlist,” the analyst revealed to Facebook that this event meant that the “user completes questionnaire marking they have been in therapy before,” thereby disclosing millions of Visitors' and Users' prior therapy to Facebook.

55. **Health information shared with other third parties:** In January 2019, Respondent disclosed to Snapchat the IP addresses and email addresses of approximately 5.6 million Visitors to re-target them with advertisements for the Service. From July 2018 to January 2019, Respondent disclosed the email addresses of over 70,000 Visitors—including Pride Counseling and Faithful Counseling Visitors—to Criteo in order to re-target them with advertisements. And, from August 2019 to September 2020, Respondent disclosed Visitors' email addresses to Pinterest for advertising.

56. **Additional use of health information for advertising:** From November 2017 to October 2020, Respondent used information concerning approximately 600,000 Pride Counseling Visitors' or Users' mental health statuses and their connection with the Visitors' and Users' LGBTQ identities to optimize future advertisements for the Service on Facebook. Respondent gathered this information through the Intake Questionnaire whenever a Pride

Counseling Visitor or User revealed that the Visitor's or User's "LGBTQ identity is contributing to your mental health concerns." Respondent used Facebook to identify characteristics and interests common among these Visitors and Users and then to target future advertisements for the Service on Facebook to individuals with similar characteristics and interests.

57. **Failure to limit third parties' use of health information:** In disclosing Visitors' and Users' health information to Facebook and other third parties, Respondent 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. For example, Facebook's Business Tools Terms, to which Respondent agreed, stated that it "may also use Event Data . . . for research and development purposes, and to . . . improve the Facebook Company Products." Similarly, Pinterest's Ad Data Terms provided: "We use Ad Data you give us for measuring ad effectiveness, ad delivery and reporting, improving safety and security on Pinterest, research and product development, and for other uses that you give us permission for." And Facebook has in fact used the Visitor and User information it received from Respondent for its own purposes, including improving its advertising products, tracking suspicious activity on its platforms, and research and development.

58. Further, though Respondent has deleted some of the Visitor and User information it disclosed to third parties from those third parties' advertising platforms, this deletion did not remove the information from those third parties' underlying databases.

### **C. Respondent's Deceptive Statements Were Material to Consumers**

59. Respondent's deceptive privacy assurances were material to consumers.

60. Visitors and Users want to keep their health information private. Indeed, a senior BetterHelp employee acknowledged at an investigational hearing conducted by FTC staff that consumers want "privacy in the context of therapy."

61. And Respondent acknowledges that this information is sensitive. In fact, Respondent's customer service representatives tell consumers that their "name, age, address, *email*, *medical history*, conversations between you and your counselor" are "PHI" or "Protected Health Information"<sup>2</sup> (emphasis added).

62. Following the February 2020 publication of news reports that Respondent was sharing consumers' health information with third parties, including Facebook, numerous Users contacted Respondent and voiced their anger about the disclosures. For example, one individual noted: "I learned that you sell yet more private information to Facebook. This is disgusting. This information makes clients easily identifiable and your platform takes 100% control of its dissemination. I have no ability to decide where that information is sent. Only you do." Another stated: "I have not given ANY consent to share my information with ANYONE. ESPECIALLY ads targeting my mental health 'weakness.'" And another called Respondent an "untrustworthy

---

<sup>2</sup> Protected Health Information is information that is considered sensitive and is protected by federal health privacy laws in certain contexts, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

company.” Other Users demanded the truth as to Respondent’s data-sharing practices, asking for assurances as to the privacy of their health information.

63. Respondent scripted the following false responses, which customer service representatives provided to Respondent’s customers: (1) “At BetterHelp, we are fully committed to protecting data and will not pass any P[ersonally] I[dentifiable] I[nformation] and/or P[rotected] H[ealth] I[nformation] to external entities including our third party partners;” and (2) “your P[rotected] H[ealth] I[nformation] and P[ersonally] I[dentifiable] I[nformation] is protected and not exposed” to Facebook.

64. Similarly, several health insurance and patient-advocacy companies representing tens of thousands of Users contacted Respondent, looking for assurance that Users’ health information had not been shared with any third parties. Senior BetterHelp employees answered each such inquiry with a variation on the same falsehood, claiming again and again that Respondent did not share any health information with any third parties.

#### **D. Respondent’s Deceptive HIPAA Seal**

65. From September 2013 to December 2020, Respondent displayed seals—in proximity to seals provided by third parties to Respondent—implying Respondent’s purported compliance with HIPAA. These seals are circled in red below:

September 2013 – December 2015:



January 2016 – December 2020:



66. By displaying the HIPAA seals on every page of the Multi-Sites, Respondent signaled to consumers that a government agency or other third party had reviewed Respondent’s privacy and information security practices and determined that they met HIPAA’s requirements. In addition, Respondent represented to consumers that it was in fact “HIPAA certified,” with its customer service representatives informing consumers that “[y]ou will also be able to see our HIPAA certification at the bottom of” our webpages.

67. However, no government agency or other third party reviewed Respondent's information practices for compliance with HIPAA, let alone determined that the practices met the requirements of HIPAA.

68. In addition, hundreds of Respondent's therapists are not subject to HIPAA and the identifiable health information of Users who engage with those therapists is therefore not protected by HIPAA. Further, Respondent does not even know which of its therapists are, or are not, subject to HIPAA, and it does not know which data are, or are not, protected by that law.

69. In December 2020, after receiving a Civil Investigative Demand from the Commission, Respondent removed the "HIPAA" seals from the Multi-Sites.

### **III. Respondent's Unfair Business Practices**

#### **A. Respondent's Unreasonable Privacy Practices**

70. From at least 2017 to at least 2021, Respondent has engaged in a number of practices that, individually or taken together, failed to safeguard Visitors' and Users' health information with respect to the collection, use, and disclosure of that information. Among other things, Respondent:

- 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 Visitors' and Users' affirmative express consent to collect, use, and disclose their health information for Respondent's 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 Visitors' and Users' health information for their own purposes, including but not limited to research and improvement of their own products, when Respondent did not provide Visitors and Users notice or obtain their consent for such uses.

71. As a result, Respondent repeatedly misrepresented its practices with respect to the collection, use, and disclosure of Visitors' and Users' health information (*see* Paragraphs 19-57, 62-64), and Respondent failed to provide consumers with sufficient notice or obtain their consent

as to these practices. Respondent disclosed these Visitors' and Users' health information to numerous third parties without authorization.

72. These misrepresentations went on for years because, until no earlier than January 2021, Respondent did nothing to ensure that its collection, use, and disclosure practices complied with their privacy promises to Visitors and Users. Indeed, neither the head of Respondent's marketing team, nor the analyst whom Respondent put in charge of advertising on Facebook reviewed the privacy policy on a regular basis, and there was no company requirement that anyone on the marketing team review the policy until no earlier than January 2021.

## **B. Injury to Consumers**

73. Respondent's collection, use, and disclosure of millions of Visitors' and Users' health information without reasonable privacy practices or safeguards has caused or is likely to cause them substantial injury. This health information—including whether Visitors and Users have previously been in therapy, the fact that they are seeking therapy or in therapy via the Service, and whether their LGBTQ status is affecting their mental health, together with identifying information such as their email addresses and IP addresses—is highly sensitive. Disclosure of this information without these Visitors' and Users' authorization is likely to cause them stigma, embarrassment, and/or emotional distress. Exposure of this information may also affect these Visitors' and Users' ability to obtain and/or retain employment, housing, health insurance, or disability insurance.

74. 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 Respondent's deceptive privacy assurances. Had Respondent 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, Respondent'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 Respondent's services. Consumers have therefore been injured by having to pay this price premium.

75. These harms were not reasonably avoidable by consumers. It was effectively impossible for Visitors and Users to know that Respondent was using and disclosing their health information for advertising purposes because Respondent actively concealed the practices through repeated misrepresentations and a lack of notice. Indeed, as described in Paragraph 62, numerous Users expressed outrage about the disclosures upon learning of them.

76. These harms were not outweighed by countervailing benefits to consumers or competition. Indeed, Respondent compromised consumers' health information for Respondent's own financial benefit through the growth of its user base, which only compounded these injuries by subjecting more Visitors and Users to Respondent's deceptive and unfair practices.

**Count I**  
**Unfairness – Unfair Privacy Practices**

77. As described in Paragraphs 16-17 and 70-72, Respondent failed to employ reasonable measures to protect consumers' health information in connection with the collection, use, and disclosure of that information, resulting in the improper and unauthorized disclosure of that information to numerous third parties for advertising and other purposes.

78. Respondent's acts or practices as set forth in Paragraph 77 caused or are likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves, as described in Paragraphs 73-76.

79. Therefore, Respondent's acts or practices as set forth in Paragraphs 77-78 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

**Count II**  
**Unfairness – Failure to Obtain Affirmative Express Consent**  
**Before Collecting, Using, and Disclosing Consumers' Health Information**

80. As described in Paragraphs 19-58, Respondent failed to obtain consumers' affirmative express consent before collecting, using, and disclosing to third parties those consumers' health information.

81. Respondent's acts or practices as set forth in Paragraph 80 caused or are likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves, as described in Paragraphs 73-76.

82. Therefore, Respondent's acts or practices as set forth in Paragraphs 80-81 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

**Count III**  
**Failure to Disclose – Disclosure of Health Information for Advertising and Third Parties' Own Uses**

83. As described in Paragraphs 41 and 44, Respondent represented, directly or indirectly, expressly or by implication, that it would disclose consumers' health information to third parties for limited purposes, and the listed purposes did not include advertising or third parties' own uses.

84. In making the representations described in Paragraph 83, Respondent failed to disclose, or failed to disclose adequately to consumers, that it disclosed consumers' health information to third parties, including Facebook, Pinterest, Snapchat, and Criteo, for advertising as well as third parties' own uses, as alleged in Paragraphs 47-57. This additional information would have been material to consumers in their decisions to use Respondent's services.

85. Therefore, Respondent's acts or practices as set forth in Paragraphs 83-84 constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

#### **Count IV**

##### **Failure to Disclose – Use of Health Information for Advertising**

86. As described in Paragraphs 41 and 44, Respondent represented, directly or indirectly, expressly or by implication, that it would use consumers' health information for limited purposes, and the listed purposes did not include advertising or advertising-related purposes.

87. In making the representations described in Paragraph 86, Respondent failed to disclose, or failed to disclose adequately to consumers, that it used consumers' health information for advertising and advertising-related purposes, as alleged in Paragraphs 46, 53, and 56. This additional information would have been material to consumers in their decisions to use Respondent's services.

88. Therefore, Respondent's acts or practices as set forth in Paragraphs 86-87 constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

#### **Count V**

##### **Privacy Misrepresentation – Disclosure of Health Information for Advertising and Third Parties' Own Uses**

89. As described in Paragraphs 28-31, 42-43, and 63-64, Respondent represented, directly or indirectly, expressly or by implication, that it would not disclose consumers' health information to any third party for advertising or that third party's own uses.

90. In fact, as set forth in Paragraphs 46-55 and 57, Respondent disclosed consumers' health information to third parties, including Facebook, Pinterest, Snapchat, and Criteo, for advertising and those third parties' own uses. Therefore, the representations set forth in Paragraph 89 are false or misleading.

91. Therefore, Respondent's acts or practices as set forth in Paragraphs 89-90 constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

#### **Count VI**

##### **Privacy Misrepresentation – Use of Health Information for Advertising**

92. As described in Paragraph 42, Respondent represented, directly or indirectly, expressly or by implication, that it would not use consumers' health information for advertising or advertising-related purposes.

93. In fact, as set forth in Paragraphs 46, 53, and 56, Respondent did use consumers' health information for advertising and advertising-related purposes. Therefore, the representations set forth in Paragraph 92 are false or misleading.

94. Therefore, Respondent's acts or practices as set forth in Paragraphs 92-93 constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

**Count VII**  
**Privacy Misrepresentation – Disclosure of Health Information**

95. As described in Paragraphs 23-26, Respondent represented, directly or indirectly, expressly or by implication, that it would not disclose consumers' health information to anyone except each consumer's licensed therapist.

96. In fact, as set forth in Paragraph 46-54, Respondent disclosed consumers' health information to at least one entity other than each consumer's licensed therapist—Facebook. Therefore, the representations set forth in Paragraph 95 are false or misleading.

97. Therefore, Respondent's acts or practices as set forth in Paragraphs 95-96 constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

**Count VIII**  
**Privacy Misrepresentation – HIPAA Certification**

98. As described in Paragraphs 65-66, Respondent represented, expressly or by implication, directly or indirectly, that a government agency or other third party had reviewed Respondent's privacy and information practices and determined that they met HIPAA's requirements.

99. In fact, as set forth in Paragraphs 67-68, no government agency or other third party had ever reviewed Respondent's privacy or information security practices and determined that they met HIPAA's requirements.

100. Therefore, Respondent's acts or practices as set forth in Paragraphs 98-99 constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this \_\_\_\_ day of \_\_\_\_\_ 2022, has issued this complaint against Respondent.

By the Commission.

April J. Tabor  
Secretary

SEAL:

# EXHIBIT B

**UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION**

**In the Matter of**

**BETTERHELP, INC., a corporation,  
also d/b/a COMPILE, INC.,  
also d/b/a MYTHERAPIST,  
also d/b/a TEEN COUNSELING,  
also d/b/a FAITHFUL COUNSELING,  
also d/b/a PRIDE COUNSELING,  
also d/b/a ICOUNSELING,  
also d/b/a REGAIN,  
also d/b/a TERAPEUTA.**

**FILE NO. 2023169**

**AGREEMENT CONTAINING  
CONSENT ORDER**

The Federal Trade Commission (the “FTC” or “Commission”) has conducted an investigation of certain acts and practices of BetterHelp, Inc. (“Proposed Respondent”). The Commission’s Bureau of Consumer Protection (“BCP”) has prepared a draft administrative Complaint (“Draft Complaint”). BCP and Proposed Respondent, individually or through its duly authorized officers, enter into this Agreement Containing Consent Order (“Consent Agreement”) to resolve the allegations in the attached Draft Complaint through a proposed Decision and Order to present to the Commission, which is also attached and made a part of this Consent Agreement.

**IT IS HEREBY AGREED** by and between Proposed Respondent and BCP, that:

1. The Proposed Respondent is BetterHelp, Inc. (“BetterHelp”), also doing business as Compile, Inc.; MyTherapist; Teen Counseling; Faithful Counseling; Pride Counseling; iCounseling; ReGain; and Terapeuta, a Delaware corporation with its principal office or place of business at 990 Villa St., Mountain View, CA 94041.
2. Proposed Respondent neither admits nor denies any of the allegations in the Draft Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Proposed Respondent admits the facts necessary to establish jurisdiction.
3. Proposed Respondent waives:
  - a. Any further procedural steps;
  - b. The requirement that the Commission’s Decision contain a statement of findings of fact and conclusions of law; and
  - c. All rights to seek judicial review or otherwise to challenge or contest the validity of the Decision and Order issued pursuant to this Consent Agreement.

4. This Consent Agreement will not become part of the public record of the proceeding unless and until it is accepted by the Commission. If the Commission accepts this Consent Agreement, it, together with the Draft Complaint, will be placed on the public record for 30 days and information about them publicly released. Acceptance does not constitute final approval, but it serves as the basis for further actions leading to final disposition of the matter. Thereafter, the Commission may either withdraw its acceptance of this Consent Agreement and so notify Proposed Respondent, in which event the Commission will take such action as it may consider appropriate, or issue and serve its Complaint (in such form as the circumstances may require) and decision in disposition of the proceeding, which may include an Order. *See* Section 2.34 of the Commission's Rules, 16 C.F.R. § 2.34 ("Rule 2.34").

5. If this agreement is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to Rule 2.34, the Commission may, without further notice to Proposed Respondent: (1) issue its Complaint corresponding in form and substance with the attached Draft Complaint and its Decision and Order; and (2) make information about them public. Proposed Respondent agrees that service of the Order may be effected by its publication on the Commission's website (ftc.gov), at which time the Order will become final. *See* Rule 2.32(d). Proposed Respondent waives any rights it may have to any other manner of service. *See* Rule 4.4.

6. When final, the Decision and Order will have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other Commission orders.

7. The Complaint may be used in construing the terms of the Decision and Order. No agreement, understanding, representation, or interpretation not contained in the Decision and Order or in this Consent Agreement may be used to vary or contradict the terms of the Decision and Order.

8. Proposed Respondent agrees to comply with the terms of the proposed Decision and Order from the date that Proposed Respondent signs this Consent Agreement. Proposed Respondent understands that it may be liable for civil penalties and other relief for each violation of the Decision and Order after it becomes final.

**BETTERHELP, INC.**

By: \_\_\_\_\_  
Kathryn Berry  
General Counsel and Vice President

Date: 11 / 21 / 2022

\_\_\_\_\_  
Phyllis Sumner  
King & Spalding  
Attorney for Proposed Respondent

Date: 11 / 21 / 2022

\_\_\_\_\_  
Marisa Maleck  
King & Spalding  
Attorney for Proposed Respondent

Date: 11 / 21 / 2022

**FEDERAL TRADE COMMISSION**

By: \_\_\_\_\_  
Miles Plant  
Attorney, Bureau of Consumer Protection

By: \_\_\_\_\_  
Manmeet Dhindsa  
Attorney, Bureau of Consumer Protection

By: \_\_\_\_\_  
Ryan Mehm  
Attorney, Bureau of Consumer Protection

**APPROVED:**

\_\_\_\_\_  
Benjamin Wiseman  
Acting Associate Director  
Division of Privacy and Identity Protection

\_\_\_\_\_  
Samuel Levine  
Director  
Bureau of Consumer Protection

2023169

**UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:**      **Lina M. Khan, Chair  
Rebecca Kelly Slaughter  
Christine S. Wilson  
Alvaro M. Bedoya**

**In the Matter of**

**BETTERHELP, INC., a corporation,  
also d/b/a COMPILE, INC.,  
also d/b/a MYTHERAPIST,  
also d/b/a TEEN COUNSELING,  
also d/b/a FAITHFUL COUNSELING,  
also d/b/a PRIDE COUNSELING,  
also d/b/a ICOUNSELING,  
also d/b/a REGAIN,  
also d/b/a TERAPPEUTA.**

**DECISION AND ORDER**

**DOCKET NO. C-**

**DECISION**

The Federal Trade Commission (the “FTC” or “Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission’s Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with

the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

### **Findings**

1. The Respondent is BetterHelp, Inc. (“BetterHelp”), also doing business as Compile, Inc.; MyTherapist; Teen Counseling; Faithful Counseling; Pride Counseling; iCounseling; ReGain; and Terappeuta, a Delaware corporation with its principal office or place of business at 990 Villa St., Mountain View, CA 94041.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

### **ORDER**

#### **Definitions**

For purposes of this Order, the following definitions apply:

- A. “Affirmative Express Consent” means any freely given, specific, informed, and unambiguous indication of an individual consumer’s wishes demonstrating agreement by the individual, such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the individual of:
  1. the categories of information that will be collected;
  2. the specific purpose(s) for which the information is being collected, used, or disclosed;
  3. the names or categories of Third Parties (e.g., “analytics partners” or “advertising partners”) collecting the information, or to whom the information is disclosed, provided that if Respondent discloses the categories of Third Parties, the disclosure shall include a hyperlink to a separate page listing the names of the Third Parties;
  4. a simple, easily located means by which the consumer can withdraw consent; and
  5. any limitations on the consumer’s ability to withdraw consent.

The Clear and Conspicuous disclosure must be separate from any “privacy policy,” “terms of service,” “terms of use,” or other similar document.

The following do not constitute Affirmative Express Consent:

1. Inferring consent from the hovering over, muting, pausing, or closing of a given piece of content by the consumer; or

2. Obtaining consent through a user interface that has the effect of subverting or impairing user autonomy, decision-making, or choice.
- B. “Clear and Conspicuous” or “Clearly and Conspicuously” means that a required disclosure is difficult to miss (*i.e.*, easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure (“triggering representation”) is made through only one means.
  2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.
  3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
  4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
  5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.
  6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
  7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
  8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, “ordinary consumers” includes reasonable members of that group.
- C. “Covered Business” means Respondent and any business that Respondent controls, directly or indirectly.
- D. “Covered Incident” means any instance of a violation of Provision I, II, or III of this Order.

- E. “Covered Information” means information from or about an individual consumer, including:
1. a first and last name;
  2. a physical address, including street name and name of city or town;
  3. geolocation information sufficient to identify street name and name of a city or town;
  4. an email address or other online contact information, such as a user identifier or a screen name;
  5. a telephone number;
  6. a government-issued identification number, such as a driver’s license, military identification, passport, Social Security number, or other personal identification number;
  7. financial institution account number;
  8. credit or debit card information;
  9. data that depicts or describes the physical or biological traits of an identified or identifiable person, including depictions, descriptions, recordings, or copies of an individual’s facial or other physical features, finger or handprints, voice, genetics, or characteristic movements or gestures;
  10. a persistent identifier, such as a customer number held in a “cookie,” a static Internet Protocol (“IP”) address, a mobile device ID, processor serial number, or any other persistent identifier that can be used to recognize a user over time and/or across different devices, websites, or online services;
  11. Treatment Information; or
  12. any individually identifiable information combined with any of (1) through (11) above.
- F. “Covered User” means any individual consumer who created an account for the online properties, services, or mobile applications associated with BetterHelp before January 1, 2021, including those properties and mobile applications associated with BetterHelp; MyTherapist; Teen Counseling; Faithful Counseling; Pride Counseling; iCounseling; Regain; and Terapeuta.
- G. “Customer” means any individual consumer who, between August 1, 2017, and December 31, 2020, signed up for and paid for the use of any online property, service, or

mobile application associated with BetterHelp, including those properties, services, and mobile applications associated with BetterHelp; MyTherapist; Teen Counseling; Faithful Counseling; Pride Counseling; iCounseling; Regain; and Terapeuta.

- H. “Delete,” “Deleted,” or “Deletion,” means to remove Covered Information such that it is not maintained in retrievable form and cannot be retrieved through physical or technical means.
- I. “Respondent” means BetterHelp, also doing business as Compile, Inc.; MyTherapist; Teen Counseling; Faithful Counseling; Pride Counseling; iCounseling; ReGain; and Terapeuta, and its successors and assigns.
- J. “Third Party” means any individual or entity other than:
  - 1. Respondent;
  - 2. a service provider of Respondent that:
    - a. processes, uses, or receives Covered Information collected by or on behalf of Respondent for and at the direction of the Respondent and no other individual or entity,
    - b. does not disclose Covered Information, or any individually identifiable information derived from such Covered Information, to any individual or entity other than Respondent or a subcontractor to such service provider bound to data processing terms no less restrictive than terms to which the service provider is bound, and
    - c. does not use Covered Information for any purpose other than performing the services specified in the service provider’s contract with Respondent;
  - 3. a therapist or counselor employed by or contracted with Respondent;
  - 4. an employee benefit program that contracts with Respondent for therapy services on behalf of the employee benefit program’s members, employees, and/or clients, provided that before Respondent may disclose any information about any of those members, employees, and/or clients to the employee benefit program, Respondent must require the employee benefit plan to obtain the authorization of the members, employees, and/or clients for such disclosure; or
  - 5. any entity (including a service provider) that uses Covered Information only as reasonably necessary to:
    - a. comply with applicable law, regulation, or legal process;
    - b. detect, prevent, or mitigate fraud or security vulnerabilities;

- c. debug to identify and repair errors that impair existing intended functionality provided that any such use is reasonably necessary and proportionate to achieve the purpose for which the Covered Information was collected or processed; or
- d. undertake internal research for the technological development and demonstration of Respondent's products or services provided that any such use is reasonably necessary and proportionate to achieve the purpose for which the Covered Information was collected or processed.

K. "Treatment Information" means individually identifiable information relating to the past, present, or future physical or mental health or condition(s) of a consumer, including:

- 1. drug, prescription, and pharmacy information;
- 2. information concerning the consumer's diagnosis;
- 3. information concerning the consumer's use of, creation of an account associated with, or response to a question or questionnaire related to, a service or product offered by Respondent or through one of any of Respondent's online properties, services, or mobile applications;
- 4. information concerning medical- or health-related purchases;
- 5. information concerning the past, present, or future payment for the provision of health care to the consumer; or
- 6. information derived or extrapolated from any of (1)-(5) above (e.g., proxy, derivative, inferred, emergent, or algorithmic data).

### **Provisions**

#### **I. Prohibition Against the Disclosure of Treatment Information and Covered Information for Certain Advertising Purposes**

**IT IS ORDERED** that Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, are prohibited from disclosing to a Third Party for the purposes of advertising, marketing, promoting, offering, offering for sale, or selling any product or service: (1) Treatment Information; and (2) Covered Information for the purpose of targeting the consumer to which the disclosed information pertains.

## **II. Affirmative Express Consent**

**IT IS FURTHER ORDERED** that, within 30 days of the effective date of this Order, Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, in connection with any product or service, prior to disclosing any consumer's Covered Information to any Third Party, must obtain the relevant consumer's Affirmative Express Consent.

## **III. Prohibition Against Misrepresentations about Privacy of Covered Information**

**IT IS FURTHER ORDERED** that Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with promoting or offering for sale any product or service must not misrepresent (or assist another in misrepresenting) in any manner, expressly or by implication:

- A. the extent to which Respondent collects, maintains, uses, discloses, Deletes, or permits or denies access to any Covered Information, or the extent to which Respondent protects the privacy, security, availability, confidentiality, or integrity of any Covered Information;
- B. the purpose(s) for which Respondent, or any entity to whom Respondent discloses or permits access to Covered Information, collects, maintains, uses, discloses, or permits access to any Covered Information;
- C. the extent to which a consumer can maintain privacy and anonymity when visiting or using any online properties, services, or mobile applications associated with Respondent;
- D. the extent to which consumers may exercise control over Respondent's collection of, maintenance of, use of, Deletion of, disclosure of, or permission of access to, Covered Information, and the steps a consumer must take to implement such controls; and
- E. the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security or any other compliance program sponsored by a government or any self-regulatory or standard-setting organization, including the Digital Advertising Alliance, the Digital Advertising Accountability Program, or any entity that certifies compliance with HIPAA; and
- F. the extent to which Respondent is a HIPAA-covered entity, and the extent that Respondent's privacy and information practices are in compliance with HIPAA requirements.

## **IV. Data Deletion**

**IT IS FURTHER ORDERED** that Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, must:

A. within 60 days after the effective date of this Order:

1. identify all Third Parties that accessed, received, or acquired Covered Information from Respondent in any form, including hashed or encrypted Covered Information, without a consumer's Affirmative Express Consent;
2. identify what Covered Information was disclosed to each Third Party identified in sub-Provision IV.A.1; and
3. submit a list of the information identified in sub-Provisions IV.A.1-2 and the methodologies used to identify the information in sub-Provisions IV.A.1-2 to: DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re BetterHelp, Inc., [X-number]."

B. within 90 days after the effective date of this Order, provide a copy of the Complaint and Order to all Third Parties identified in sub-Provision IV.A.1, notify all such Third Parties in writing that the Federal Trade Commission alleges that Respondent disclosed Covered Information of consumers to them in a manner that was unfair or deceptive and in violation of the FTC Act, and instruct those Third Parties to Delete all Covered Information accessed, received, or acquired from Respondent without a consumer's Affirmative Express Consent. Respondent's instruction to each such Third Party shall include a list of the Covered Information identified in sub-Provision IV.A.2 and shall demand written confirmation from each such Third Party that it has Deleted such Covered Information. Respondent must provide all instructions sent to the Third Parties to: DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re BetterHelp, Inc., [X-number]"

C. as of the issuance of this Order:

1. Respondent shall not disclose any Covered Information in any form, including hashed or encrypted Covered Information, to any Third Party identified in sub-Provision IV.A.1 until Respondent confirms each Third Party's receipt of the instructions required by sub-Provision IV.B. This sub-Provision is subject to the prohibitions set forth in Provision I. Respondent must provide all receipts of confirmation and any responses from Third Parties within five (5) days of receipt to: DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re BetterHelp, Inc., [X-number]."

2. Respondent shall not use any Third Party identified in sub-Provision IV.A.1 to advertise, market, promote, offer, offer for sale, or sell any product or service until Respondent confirms each Third Party's receipt of the instructions required by sub-Provision IV.B.

## V. Notice to Users

**IT IS FURTHER ORDERED** that, on or before 14 days after the effective date of this Order, Respondent must email all Covered Users, using the last known verified email address in Respondent's possession, custody, or control, an exact copy of the notice attached hereto as Exhibit A ("Notice"), *provided however*, that if Respondent does not have email information for any Covered User, Respondent must send the Notice to that Covered User through Respondent's primary means of communicating with that user. Respondent shall not include with the Notice any other information, documents, or attachments.

## VI. Mandated Privacy Program

**IT IS FURTHER ORDERED** that any Covered Business, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must, within 60 days of the effective date of this Order, establish and implement, and thereafter maintain, a comprehensive privacy program ("Privacy Program") that protects the privacy, security, availability, confidentiality, and integrity of such Covered Information. To satisfy this requirement, Respondent must, for each Covered Business, at a minimum:

- A. document in writing the content, implementation, and maintenance of the Privacy Program;
- B. provide the written program and any evaluations thereof or updates thereto to the Covered Business's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of the Covered Business responsible for the Covered Business's Privacy Program at least once every 12 months and promptly (not to exceed 30 days) after a Covered Incident;
- C. designate a qualified employee or employees, who report(s) directly to an executive, such as the Chief Executive Officer, Chief Compliance Officer, or Chief Legal Officer, to coordinate and be responsible for the Privacy Program; and keep the executive and the Board of Directors informed of the Privacy Program, including all actions and procedures implemented to comply with the requirements of this Order, and any actions and procedures to be implemented to ensure continued compliance with this Order;
- D. assess and document, at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, internal and external risks in each area of the Covered Business's operations to the privacy, security, availability, confidentiality, and integrity of Covered Information that could result in the unauthorized access, collection, use, destruction, or disclosure of, or provision of access to, Covered Information;

- E. design, implement, maintain, and document safeguards that control for the internal and external risks to the privacy, security, availability, confidentiality, and integrity of Covered Information identified by the Covered Business in response to sub-Provision VI.D. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, Deletion, disclosure of, or provision of access to, the Covered Information. Such safeguards must also include:
1. policies, procedures, and technical measures to systematically inventory Covered Information in the Covered Business's control and Delete Covered Information that is no longer reasonably necessary and in accordance with applicable retention laws and regulations;
  2. policies, procedures, and technical measures to prevent the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information inconsistent with the Covered Business's representations to consumers;
  3. audits, assessments, and reviews of the contracts, privacy policies, and terms of service associated with any Third Party to which the Covered Business discloses, or provides access to, Covered Information;
  4. policies and technical measures that limit employee and contractor access to Covered Information to only those employees and contractors with a legitimate business need to access such Covered Information;
  5. mandatory privacy training programs for all employees on at least an annual basis, updated to address the collection, use, and disclosure of Covered Information for advertising purposes; any internal or external risks identified by Respondent in sub-Provision VI.D; and safeguards implemented pursuant to sub-Provision VI.E, that include training on the requirements of this Order;
  6. a data retention policy that, at a minimum, includes:
    - a. a retention schedule that limits the retention of Covered Information for only as long as is necessary to fulfill the purpose for which the Covered Information was collected; provided, however, that such Covered Information need not be Deleted, and may be disclosed, to the extent requested by a government agency or required by law, regulation, or court order; and
    - b. a requirement that Respondent documents, adheres to, and makes publicly available on its terms of service/use a retention schedule for Covered Information, setting forth: (1) the purposes for which the Covered Information is collected; (2) the specific business need for retaining each type of Covered Information; and (3) a set timeframe in accordance with applicable laws and regulations for Deletion of each type of Covered Information (absent any intervening Deletion requests from consumers) that precludes indefinite retention of any Covered Information;

7. for each product or service, policies and procedures to document internally the decision to collect, use, Delete, disclose, or provide access to, each type of Covered Information. Such documentation should include: (a) the name(s) of the person(s) who made the decision; (b) for what purpose the type of Covered Information is being collected; (c) the data segmentation controls in place to ensure that the Covered Information collected is only used and/or disclosed for the particular purpose(s) for which it was collected; (d) the data retention limit set and the technical means for achieving Deletion; (e) the safeguards in place to prevent unauthorized disclosure of each type of Covered Information; and (f) the access controls in place to ensure only authorized employees with a need-to-know have access to the Covered Information;
  8. audits, assessments, reviews, or testing of each mechanism by which the Covered Business discloses Covered Information to a Third Party or provides a Third Party with access to Covered Information (including but not limited to web beacons, pixels, and Software Development Kits); and
  9. for each product or service offered by any Covered Business, Clearly and Conspicuously disclose the categories of Covered Information collected from consumers, the purposes for the collection of each category of Covered Information, and any transfer of Covered Information to a Third Party. For each such transfer of Covered Information, the disclosure must, at a minimum, include: (a) the specific categories of Covered Information transferred; (b) the identity of each Third Party receiving the transfer; (c) the purposes for which the Covered Business transferred the Covered Information; (d) the purposes for which each Third Party receiving the Covered Information may use the Covered Information, including but not limited to the purposes for the Third Party reserves the right to use such Covered Information; and (e) whether each Third Party receiving the transfer of Covered Information reserves the right to transfer the Covered Information to other entities or individuals.
- F. assess, at least once every 12 months, and promptly (not to exceed 30 days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, availability, confidentiality, and integrity of Covered Information, and modify the Privacy Program based on the results;
  - G. test and monitor the effectiveness of the safeguards at least once every 12 months, and promptly (not to exceed 30 days) following a Covered Incident, and modify the Privacy Policy based on the results;
  - H. select and retain service providers capable of safeguarding Covered Information they receive from the Covered Business, and contractually require service providers to implement and maintain safeguards for Covered Information; and
  - I. evaluate and adjust the Privacy Program in light of any material changes to the Covered Business's operations or business arrangements, the results of the testing and monitoring required by sub-Provision VI.G, a Covered Incident, and any other circumstances that the

Covered Business knows or has reason to believe may have a material impact on the effectiveness of the Privacy Program or any of its individual safeguards (including but not limited to new or more efficient technological or operational methods to control for the risks identified in sub-Provision VI.D). The Covered Business may make this evaluation and adjustment to the Privacy Program at any time, but must, at a minimum, evaluate the Privacy Program at least once every 12 months and modify the Privacy Program as necessary based on the results.

## **VII. Privacy Assessments by a Third-Party Assessor**

**IT IS FURTHER ORDERED** that, in connection with its compliance with Provision VI, for any Covered Business that collects, maintains, uses, discloses, or provides access to Covered Information, Respondent must obtain initial and biennial assessments (“Assessments”):

- A. The Assessments must be obtained from a qualified, objective, independent third-party professional (“Assessor”), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Privacy Program; (3) retains all documents relevant to each Assessment for 5 years after completion of such Assessment; and (4) will provide such documents to the Commission within 10 days of receipt of a written request from a representative of the Commission. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim. The Assessor must have a minimum of 3 years of experience in the field of privacy and data protection.
- B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in his or her sole discretion.
- C. The reporting period for the Assessments must cover: (1) the first 240 days after the issuance date of the Order for the initial Assessment; and (2) each 2-year period thereafter for 20 years after the issuance date of the Order for the biennial Assessments.
- D. Each Assessment must, for the entire assessment period:
  1. determine whether Respondent has implemented and maintained the Privacy Program required by Provision VI;
  2. assess the effectiveness of Respondent’s implementation and maintenance of sub-Provisions VI.A-I;
  3. identify any gaps or weaknesses in the Privacy Program, or instances of material noncompliance with, sub-Provisions VI.A-I;

4. address the status of gaps or weaknesses in the Privacy Program, as well as any instances of material non-compliance with sub-Provisions VI.A-I, that were identified in any prior Assessment required by this Order; and
  5. identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely solely on assertions or attestations by Respondent, Respondent's management, or a Covered Business's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Privacy Program and did not rely solely on assertions or attestations by Respondent, Respondent's management, or a Covered Business's management, and state the number of hours that each member of the Assessor's assessment team worked on the Assessment. To the extent a Covered Business revises, updates, or adds one or more safeguards required under sub-Provision VI.E in the middle of an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.
- E. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within 10 days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re BetterHelp, Inc., [X-number]." All subsequent biennial Assessments must be retained by Respondent until the Order is terminated and provided to the Associate Director for Enforcement within 10 days of request.

### **VIII. Cooperation with Assessor**

**IT IS FURTHER ORDERED** that Respondent, whether acting directly or indirectly, in connection with the Assessments required by Provision VII, must:

- A. provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;
- B. provide or otherwise make available to the Assessor information about all Covered Information in Respondent's custody or control so that the Assessor can determine the scope of the Assessment; and

- C. disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Privacy Program required by Provision VI; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions VI.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Privacy Program required by Provision VI.

### **IX. Annual Certification**

**IT IS FURTHER ORDERED** that Respondent must:

- A. one year after the issuance date of this Order, and each year thereafter for 10 years, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of each Covered Business that: (1) the Covered Business has established, implemented, and maintained the requirements of this Order; (2) the Covered Business is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of any Covered Incident. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.
- B. unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re BetterHelp, Inc., [X-number]."

### **X. Covered Incident Reports**

**IT IS FURTHER ORDERED** that Respondent, within 30 days after Respondent's discovery of a Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

- A. the date, estimated date, or estimated date range when the Covered Incident occurred;
- B. a description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;
- C. the number of consumers whose information was affected;
- D. the acts that Respondent has taken to date to remediate the Covered Incident; protect Covered Information from further disclosure, exposure, or access; and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

- E. a representative copy of any materially different notice sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: “In re BetterHelp, Inc., [X-number].”

## **XI. Monetary Relief**

**IT IS FURTHER ORDERED** that:

- A. Respondent must pay to the Commission \$7,800,000, which Respondent stipulates its undersigned counsel holds in escrow for no purpose other than payment to the Commission.
- B. Such payment must be made within 8 days of the effective date of this Order by electronic fund transfer in accordance with instructions provided by a representative of the Commission.

## **XII. Additional Monetary Provisions**

**IT IS FURTHER ORDERED** that:

- A. Respondent relinquishes dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the return of any assets.
- B. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Commission to enforce its rights to any payment pursuant to this Order, such as a nondischargeability complaint in any bankruptcy case.
- C. The facts alleged in the Complaint establish all elements necessary to sustain an action by or on behalf of the Commission pursuant to Section 523(a)(2)(A) of the Bankruptcy Code, 11 U.S.C. § 523(a)(2)(A), and this Order will have collateral estoppel effect for such purposes.
- D. All money paid to the Commission pursuant to this Order may be deposited into a fund administered by the Commission or its designee to be used for relief, including consumer redress and any attendant expenses for the administration of any redress fund. If a representative of the Commission decides that direct redress to consumers is wholly or partially impracticable or money remains after redress is completed, the Commission may apply any remaining money for such other relief (including consumer information remedies) as it determines to be reasonably related to Respondent’s practices alleged in

the Complaint. Any money not used is to be deposited to the U.S. Treasury. Respondent has no right to challenge any activities pursuant to this Provision.

- E. All decisions regarding the administration and amount of redress provided shall be made by the Commission in its sole discretion; however, the names and identifying information of all consumers who receive redress shall be provided solely to the Redress Administrator pursuant to Provision XIII.
- F. In the event of default on any obligation to make payment under this Order, interest, computed as if pursuant to 28 U.S.C. § 1961(a), shall accrue from the date of default to the date of payment. In the event such default continues for 10 days beyond the date that payment is due, the entire amount will immediately become due and payable.
- G. Each day of nonpayment is a violation through continuing failure to obey or neglect to obey a final order of the Commission and thus will be deemed a separate offense and violation for which a civil penalty shall accrue.
- H. Respondent acknowledges that its Taxpayer Identification Numbers (Social Security or Employer Identification Numbers), which Respondent has previously submitted to the Commission, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. § 7701.

### **XIII. Independent Redress Administrator**

**IT IS FURTHER ORDERED** that an independent redress administrator (“Administrator”) shall be appointed to assist with the efficient administration of consumer redress:

- A. Commission staff, in their sole discretion, shall select the Administrator, who shall be an independent third party, not an employee of the Commission or Respondent.
- B. Within 7 days of entry of this Order, Respondent must provide the Administrator with all information necessary to identify all Customers and all information necessary for the efficient administration of consumer redress to those Customers. Respondent stipulates it has provided such information to its undersigned counsel. If a representative of the Commission or the Administrator requests any additional information related to consumer redress, Respondent must provide it, in the form prescribed by the Commission or the Administrator, within 14 days of the request, provided that, any request for personally identifying Customer information shall be directed solely to the Administrator.
- C. The Administrator shall be responsible for reviewing, assessing, and evaluating the Customer information for consumer redress, and for ensuring the efficient administration of consumer redress as follows:
  - 1. The Administrator shall receive, review, and assess the Customer information provided by Respondent to ensure it is sufficient for the efficient administration of

consumer redress as determined by the Commission. If a representative of the Commission requests any additional information related to redress, the Administrator must provide it, in the form prescribed by the Commission, within 14 days, provided however, that the Administrator may not share personally identifying Customer information with the Commission.

2. Within 45 days of entry of this Order, the Administrator shall confirm in writing that it has a complete list of Customers, or that the Administrator does not and why not.
  3. The Administrator is responsible for conducting supplemental address searches or other inquiries related to consumer redress if the Commission or the Administrator determines it necessary or advisable.
  4. The Administrator is authorized to choose, engage, and employ service providers as the Administrator deems advisable or necessary in the performance of the Administrator's duties and responsibilities under the authority granted by this Order. The Administrator may only employ service providers capable of safeguarding Customer information they receive from the Administrator, and the Administrator must contractually require service providers to implement and maintain safeguards for such Customer information.
  5. The Administrator shall administer consumer redress as specified by the Commission. The Administrator must follow all instructions dictated by the Commission for the efficient administration of consumer redress, including but not limited to instructions pertaining to consumer communications and redress process and distributions.
  6. The Administrator must cooperate with the Commission to request the transfer of funds necessary for consumer redress distribution.
  7. No later than three months after the date on which the Administrator is retained, and every three months thereafter until such time the Commission determines the administration of consumer redress has concluded, the Administrator shall submit a report to the Commission concerning the status of consumer redress and detailing the progress of the administration of consumer redress, including but not limited to the amounts of funds distributed for redress payment, the consumer participation rate, the length of time for consumers to receive redress payment, and any complaints received regarding consumer redress.
- D. Respondent shall fully cooperate with and assist the Administrator. That cooperation and assistance shall include, but not be limited to, providing information to the Administrator as the Administrator deems necessary to be fully informed and discharge the responsibilities of the Administrator under this Order. For matters concerning this Order, the Administrator is authorized to communicate directly with Respondent.

- E. Respondent is responsible for all costs and fees invoiced by the Administrator for its services, and the provision of consumer redress. The FTC is not responsible for any such costs or fees. None of the funds used to satisfy Provision XI of this Order shall be used to pay for the Administrator or any of its associated costs or fees.

#### **XIV. Acknowledgments of the Order**

**IT IS FURTHER ORDERED** that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For 10 years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in Provision XV. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondent delivered a copy of this Order, that Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

#### **XV. Compliance Reports and Notices**

**IT IS FURTHER ORDERED** that Respondent makes timely submissions to the Commission:

- A. One hundred and eighty days after the effective date of this Order, and annually thereafter for five more years, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of that Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the services offered, the means of advertising and marketing, what Covered Information it collects, how Covered Information is used and disclosed to Third Parties; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in: (a) any designated point of contact; or (b) the structure of any Covered Business, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within 14 days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: \_\_\_\_\_” and supplying the date, signatory’s full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: “In re BetterHelp, Inc., [X-number].”

## **XVI. Recordkeeping**

**IT IS FURTHER ORDERED** that Respondent must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years, unless otherwise specified below. Specifically, Respondent for each Covered Business, must create and retain the following records:

- A. accounting records showing the revenues from all products or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;
- B. personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person’s: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. copies or records of all consumer complaints and refund requests concerning the collection, use, maintenance, disclosure, deletion, or permission of access to Covered Information, whether received directly or indirectly, such as through a Third Party, and any response;
- D. records of all disclosures of consumers’ Covered Information to Third Parties showing, for each Third Party that received Covered Information, the name and address of the Third Party, the date(s) of such disclosures, the purpose(s) for which the Covered

Information was transferred, and how and when Respondent obtained consumers' Affirmative Express Consent for the disclosures in accordance with Provision II;

- E. a copy of each unique advertisement or other marketing material making a representation subject to this Order;
- F. a copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, security, availability, confidentiality, or integrity of any Covered Information, including any representation concerning a change in any website or other service controlled by Respondent that relates to the privacy, security, availability, confidentiality, or integrity of Covered Information;
- G. for 5 years after the date of preparation of each Assessment required by Provision VII, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment;
- H. for 5 years from the date received, copies of all subpoenas and other communications with law enforcement, if such communication relate to Respondent's compliance with this Order;
- I. for 5 years from the date created or received, all records, whether prepared by or on behalf of Respondent, that tend to show any lack of compliance by Respondent with this Order; and
- J. all records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

## **XVII. Compliance Monitoring**

**IT IS FURTHER ORDERED** that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within 10 days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 & 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

### **XVIII. Order Effective Dates**

**IT IS FURTHER ORDERED** that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. any Provision in this Order that terminates in less than 20 years;
- B. this Order's application to Respondent that is not named as a defendant in such complaint; and
- C. this Order if such complaint is filed after the Order has terminated pursuant to this Provision.

*Provided, further*, that if such complaint is dismissed or a federal court rules that Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor  
Secretary

SEAL:  
ISSUED:

## **Exhibit A**

### Notice to Covered Users

[Subject: The Federal Trade Commission Alleges That We Shared Information About You Without Your Permission]

[To appear with the BetterHelp logo]

Hello,

We are contacting you because you used BetterHelp's services (or its partner services Pride Counseling, Teen Counseling, Faithful Counseling, iCounseling, ReGain, or Terapeuta) or created an account for one of these services between January 2013 and December 2020. When you used our services, we promised to keep your personal health information private. The Federal Trade Commission ("FTC") alleges that we shared health information about you to other companies without your approval.

### **What happened?**

The FTC alleges that we shared information about you, including information that could be used to identify you, with Facebook, Inc. (now "Meta"); Snapchat (Snap Inc.); Pinterest; and/or Criteo. The FTC alleges that this information may have included:

- Your hashed email address, which these companies used to identify you if you had an account with them
- The IP address that may identify your device when you access our service
- If you answered "yes" to the Intake Questionnaire question "Have you ever been in therapy before?"
- If you answered "good" or "fair" to the Intake Questionnaire question "How would you rate your current financial status?"

The FTC alleges that, in many cases, the companies we shared your information with linked it with your accounts on their platforms so we could show ads to you or people like you.

We didn't share your messages, transcripts of conversations, sessions data, journal entries, worksheets, or any other type of communications between you and your therapist with these companies.

### **What are we doing in response?**

We have entered into an agreement with the FTC relating to the sharing of this information. To resolve the case:

- We'll tell the advertising companies that received your information to delete it.
- We aren't sharing your health information with other companies for advertising anymore. And we aren't sharing your personal information for advertising without your permission.
- We'll enhance our privacy program to better protect your personal health information. An independent third party will audit our program to make sure we're protecting your information. These audits will happen every two years for the next 20 years.

### **Learn more**

If you have any questions, email us at [email address].

To learn more about the settlement, go to [ftc.gov](https://www.ftc.gov) and search for "BetterHelp."

For advice on protecting your health privacy, read the FTC's [Does your health app protect your sensitive info?](#)

2023169

**UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:**      **Lina M. Khan, Chair**  
                                 **Rebecca Kelly Slaughter**  
                                 **Christine S. Wilson**  
                                 **Alvaro M. Bedoya**

**In the Matter of**

**BETTERHELP, INC., a corporation,  
also d/b/a  
COMPILE, INC.,  
also d/b/a MYTHERAPIST,  
also d/b/a TEEN COUNSELING,  
also d/b/a FAITHFUL COUNSELING,  
also d/b/a PRIDE COUNSELING,  
also d/b/a ICOUNSELING,  
also d/b/a REGAIN,  
also d/b/a TERAPEUTA.**

**DOCKET NO.**

**COMPLAINT**

The Federal Trade Commission (“FTC” or “Commission”), having reason to believe that BetterHelp, Inc., a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent BetterHelp, Inc. (“BetterHelp” or “Respondent”), also doing business as Compile, Inc.; MyTherapist; Teen Counseling; Faithful Counseling; Pride Counseling; iCounseling; ReGain; and Terapeuta, is a Delaware corporation with its principal office or place of business at 990 Villa Street, Mountain View, CA 94041.
2. Respondent has developed, advertised, and offered for sale an online counseling service (the “Service”)—including specialized versions of the Service for people of the Christian faith, members of the LGBTQ community, and teenagers—which matches users with Respondent’s therapists and then facilitates counseling via Respondent’s websites and apps.
3. Millions of consumers have signed up for the Service, entrusting Respondent with their email addresses, IP addresses, and certain information about their health status and histories—such as the fact that they are seeking or are in therapy, and whether they have previously been in therapy. Because Respondent collects certain types of personal information from consumers when they take affirmative steps to sign up for the Service, Respondent’s disclosure of that information to a third party would implicitly disclose the consumer’s interest in or use of the

Service and therefore constitute a disclosure of the consumer's health information. For example, because Respondent obtained a consumer's email address only when the consumer took affirmative steps to utilize the Service, Respondent's disclosure of this information would identify the consumer as associated with seeking and/or receiving mental health treatment. Similarly, Respondent's disclosure that a consumer took affirmative steps to sign up for the Service (such as by filling out Respondent's intake questionnaire for the Service or becoming a paying user), along with an identifier (for example, an IP address), would disclose the consumer's seeking of mental health treatment via the Service.

4. Recognizing the sensitivity of this health information, Respondent has repeatedly promised to keep it private and use it only for non-advertising purposes such as to facilitate consumers' therapy.

5. From 2013 to December 2020, however, Respondent continually broke these privacy promises, monetizing consumers' health information to target them and others with advertisements for the Service. For example, from 2018 to 2020, Respondent used these consumers' email addresses and the fact that they had previously been in therapy to instruct Facebook to identify similar consumers and target them with advertisements for the Service, bringing in tens of thousands of new paying users, and millions of dollars in revenue, as a result.

6. To capitalize on these consumers' health information, Respondent handed it over to numerous third-party advertising platforms, including Facebook, Pinterest, Snapchat, and Criteo, often permitting these companies to use the information for their own research and product development as well.

7. In addition, Respondent failed to employ reasonable measures to safeguard the health information it collected from consumers. In particular, Respondent did not properly train its employees on how to protect the information when using it for advertising, and Respondent did not properly supervise its staff in the use of the information. Respondent also failed to provide consumers with proper notice as to the collection, use, and disclosure of their health information. And Respondent failed to limit contractually how third parties could use consumers' health information, instead merely agreeing to their stock contracts and terms.

8. It was only in December 2020, well after reporters brought these practices to light and the FTC began investigating the practices, that Respondent curtailed its unauthorized use and disclosure of consumers' health information.

9. The acts and practices of Respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

## **I. Background**

### **A. The Service**

10. Respondent offers the Service under several names, each of which has its own website and app (collectively, the "Multi-Sites"). Its primary website and app, which is named "BetterHelp," serves general audiences and has been in operation since 2013. Faithful Counseling, in operation since July 2017, is aimed at consumers of the Christian faith. Pride

Counseling, in operation since August 2017, caters to the LGBTQ community. Teen Counseling, in operation since January 2017, offers counseling to 13- to 18-year-olds with parental consent. And ReGain, in operation since May 2016, offers couples counseling.<sup>1</sup> The Multi-Sites all function similarly and facilitate therapy via the Service, and they are all subject to Respondent's policies, practices, and procedures.

11. Users pay \$60 to \$90 per week for counseling through the Service. To sign up for the Service and become a paying user (a "User"), an individual visiting one of the Multi-Sites (a "Visitor") must fill out a questionnaire (the "Intake Questionnaire"), answering detailed questions about the Visitor's mental health.

12. Upon completing the Intake Questionnaire, a Visitor is prompted to create an account for the Service by entering the Visitor's name or nickname, email address, phone number, and emergency contact information. The Visitor is then asked to enter credit card information to become a paying User.

13. Respondent then utilizes the User's responses to the Intake Questionnaire to match the User with one of Respondent's more than 25,000 licensed therapists. Respondent's therapists provide Users with mental health therapy via video conferencing, text messaging, live chat, and audio calls.

14. Respondent's primary website and app, "BetterHelp," has seen explosive growth over the last few years, 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, and, today, it has over 374,000 active Users in the United States. As a result, Respondent earned over \$345 million in revenue in 2020, and over \$720 million in revenue in 2021.

## **B. Respondent's Marketing History**

15. Since its inception, Respondent has utilized numerous third parties to market the Service, including, at various times, Facebook, Snapchat, Pinterest, and Criteo. In addition, Respondent has advertised the Service on search engines, television, podcasts, and radio.

16. In 2017, Respondent delegated most decision-making authority over its use of Facebook's advertising services to a Junior Marketing Analyst who was a recent college graduate, had never worked in marketing, and had no experience and little training in safeguarding consumers' health information when using that information for advertising. In doing so, Respondent gave the Junior Marketing Analyst carte blanche to decide which Visitors' and Users' health information to upload to Facebook and how to use that information. This same individual, who now holds the title "Senior Marketing Analyst," continues to oversee Respondent's use of Facebook's advertising tools.

17. Respondent provided this marketing analyst with little training on how to protect Visitors' and Users' health information in connection with advertising until 2021. In fact, while

---

<sup>1</sup> Respondent also offered the Service through the iCounseling website and app from February 2017-November 2020, the Terapeuta website and app from March 2017-March 2019, and the MyTherapist website and app from June 2017-March 2019.

Respondent has purported to provide privacy training to its employees since 2015, it was not until 2021 that Respondent gave them any training specific to its business or advertising.

18. Respondent has spent tens of millions of dollars annually to market the Service. In 2020, for example, it spent \$10-\$20 million on Facebook advertising, and by 2021 Respondent's advertising on Facebook was bringing in approximately 30,000 to 40,000 new Users per quarter.

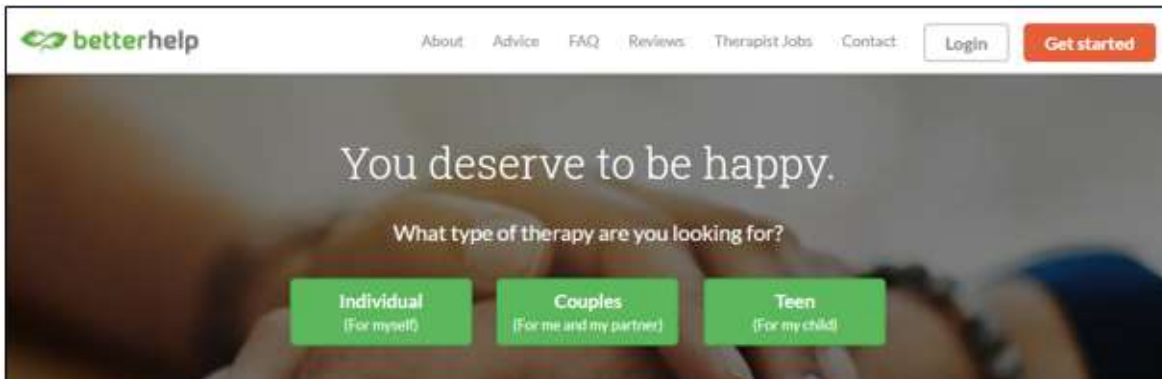
## **II. Respondent's Deceptive Business Practices**

19. In connection with the advertisement and sale of the Service, Respondent has disseminated, or caused to be disseminated, false and deceptive statements about its use and disclosure of consumers' health information. Respondent also disseminated, or caused to be disseminated, misleading and deceptive representations regarding its compliance with federal health privacy laws. Visitors and Users relied on these representations and were misled as a result.

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

#### Respondent's deceptive statements concerning Intake Questionnaire responses

20. Upon arriving at any of the Multi-Sites, a Visitor is immediately prompted to begin the 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:



21. After making a selection, the Visitor is ushered through the Intake Questionnaire, which asks an array of questions. For many Visitors, these questions include whether the Visitor is "experiencing overwhelming sadness, grief, or depression"; whether the Visitor has been having thoughts that the Visitor "would be better off dead or hurting yourself in some way"; whether the Visitor is "currently taking any medication"; whether the Visitor has "problems or worries about intimacy"; and whether the Visitor has previously been in therapy.


22. The Intake Questionnaire also asks whether the Visitor identifies as a member of the Christian faith, shuttling such individuals to Faithful Counseling. Similarly, the Intake Questionnaire takes those who identify as members of the LGBTQ community to Pride

Counseling. And Respondent ushers teenagers to Teen Counseling, where the teenage Visitors provide their responses to the Intake Questionnaire before Respondent obtains parental consent.

23. Respondent has included privacy assurances throughout the Intake Questionnaire. Until November 2021, each Multi-Site displayed a banner at the top of each question, explaining that Respondent 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 Visitor can be matched “with the most suitable therapist for you.”

24. As Visitors proceed through the Intake Questionnaire, Respondent includes additional periodic privacy assurances. From at least August 2017 to December 2020, when a Visitor reached the question as to whether the Visitor was taking medication, the Visitor was shown the statement: “Rest assured—any information provided in this questionnaire will stay private between you and your counselor.”

25. In December 2020, Respondent changed the statement to read: “Rest assured—*this information* will stay private between you and your counselor” (emphasis on alteration added). And in January 2021, Respondent changed it again to state: “Rest assured—*your health information* will stay private between you and your counselor” (emphasis on alteration added). This version, which was in use until September 2021, is circled in red below:



Are you currently taking any medication?

No

Yes

 Rest assured - your health information will stay private between you and your counselor.

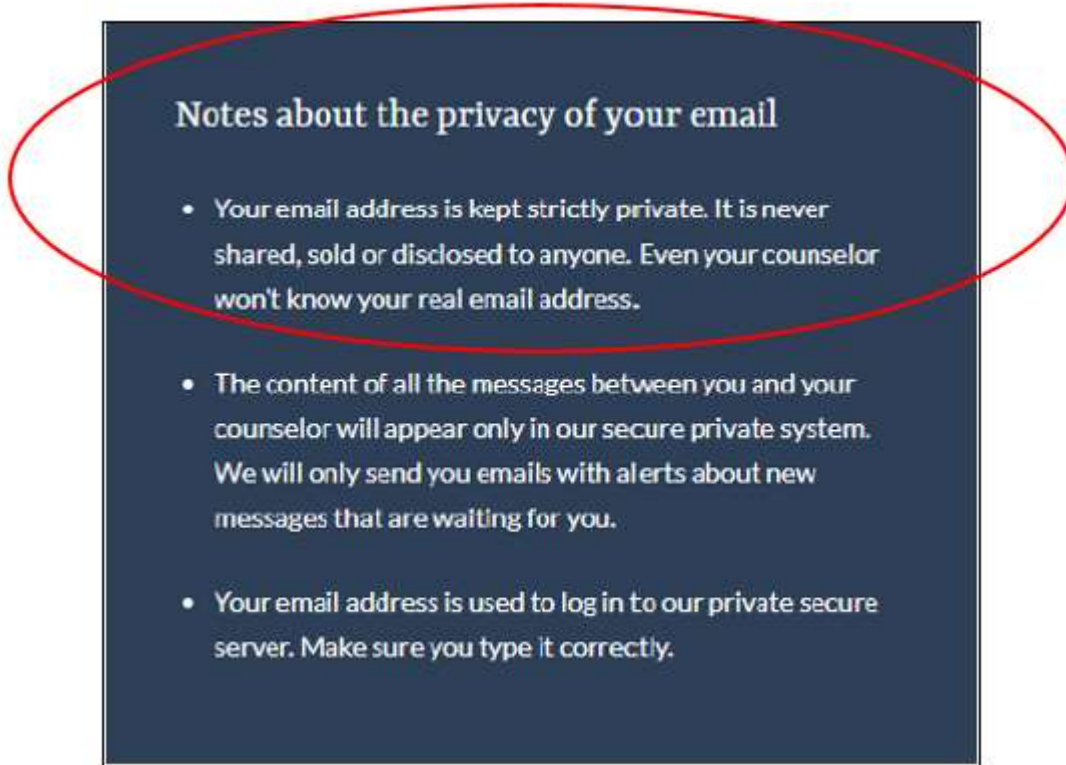
In October 2021, Respondent removed this representation altogether.

26. After being presented with these repeated promises of privacy, millions of Visitors, including those that became Users, filled out the Intake Questionnaire and shared their health information with Respondent.

27. Despite the aforementioned assurances of privacy, Respondent disclosed Visitors’ and 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 discussed in Paragraphs 51-54 and 57 below.

Respondent falsely promised to keep Christian, LGBTQ, and teenage consumers' email addresses "strictly private"

28. From at least August 2017 to as recently as December 2020, Respondent gave additional privacy assurances to Faithful Counseling, Pride Counseling, and Teen Counseling Visitors to induce them to sign up for the Service, stating that their email addresses would be "kept strictly private" and "never shared, sold or disclosed to anyone." This representation, which Respondent displayed prominently and unavoidably during the sign-up process, is circled in red below:



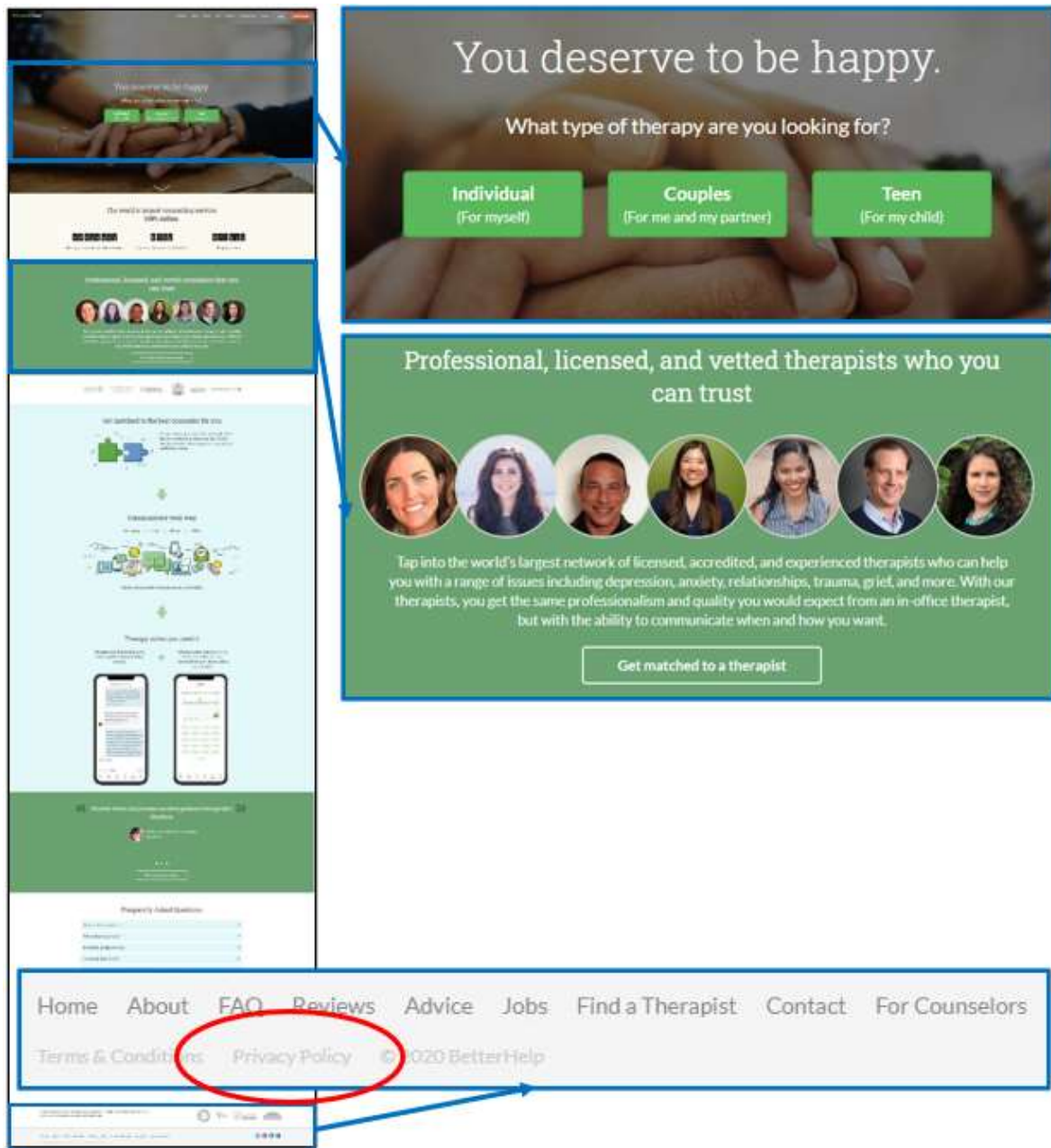
29. Tens of thousands of Visitors provided Respondent with their email addresses and signed up for Faithful Counseling, Pride Counseling, and Teen Counseling after viewing this privacy assurance.

30. Respondent understood that its disclosure of Visitors' email addresses in association with BetterHelp would reveal that the Visitors were seeking mental health treatment through the Service. And Respondent understood that consumers would want to keep this information private. In fact, a senior BetterHelp employee acknowledged at an investigational hearing conducted by FTC staff that individuals "want to keep . . . the fact that they're in therapy private" and at times even "keep their identities . . . secret from their therapist[s]."

31. Nevertheless, Respondent disclosed the email addresses of thousands of these Visitors to various third parties for advertising purposes and the third parties' own purposes, as discussed in further detail in Paragraphs 47-55 and 57, thereby revealing to the third parties that these Visitors were seeking and/or receiving mental health treatment via the Service.

Respondent pushed Visitors and Users into disclosing their health information

32. In addition to making false representations, Respondent has pushed Visitors and Users into handing over their health information before they have ever had a chance to read any privacy disclosures.
33. Upon visiting any of the Multi-Sites, Visitors are urged to begin the Intake Questionnaire and hand over their health information. At the same time, Visitors are repeatedly presented with the aforementioned privacy assurances discussed in Paragraphs 23-25 and 28—displayed in large, high-contrast, unavoidable text.
34. By contrast, Respondent linked to the privacy policy in small, low-contrast writing that is barely visible at the bottom of the page.
35. The image below depicts the BetterHelp homepage ([www.betterhelp.com](http://www.betterhelp.com)), with the prompts to enter the Intake Questionnaire magnified at the top and the link to the privacy policy magnified at the bottom and circled in red:



36. In September 2020, Respondent added the below banner to the bottom of every page of its Multi-Sites (until a Visitor closed it), which stated: “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.”



37. Despite including a link to the privacy policy, the banner effectively dissuaded Visitors from reading the privacy policy by stating, until October 2020, that Respondent would “never sell or rent any information you share with us.”

38. In May 2021, Respondent revised the banner and added 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). But this banner still did not inform Visitors that Respondent would use and disclose their health information for advertising or that third parties would be able to use Visitors’ information for their own purposes.

39. It was not until October 2021 that Respondent revised the banner to state that it discloses Visitors’ IP addresses and other personal identifiers for advertising and offered Visitors an opportunity to opt out of the disclosures via the banner.

Respondent’s privacy policies claimed limited use and disclosure of consumers’ information

40. Those Visitors and Users that persevered and read Respondent’s privacy policy were presented with additional deceptive statements about Respondent’s use and disclosure of health information.

41. From August 2013 to November 2018, Respondent’s privacy policies represented that it would use and disclose Visitors’ and Users’ 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. Notably, these privacy policies made no mention of using or disclosing this information for advertising purposes, and they said nothing about permitting third parties to use this information for their own purposes.

42. In November 2018, Respondent 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. These limited purposes did not include using or disclosing the information for advertising or disclosing the information to third parties for their own purposes.

43. Respondent revised its privacy policy again in September 2019, stating that it might *use* this health information for advertising. But the policy continued to say that Respondent 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, Respondent revised the privacy policy yet again, finally stating that it may *both use and disclose* Visitors’ and Users’ information for advertising. But, even then, the privacy policy continued to claim that Respondent would disclose this information to third parties for only the stated limited purposes, which did not include third parties’ own purposes.

44. 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 Visitors’ or Users’ health information for advertising purposes, or the disclosure of this information for third parties’ own purposes. These tools allow

Respondent and third parties to collect Visitors' and Users' information when they use one of the Multi-Sites, including what pages a Visitor or User visits and what information a Visitor or User inputs into the website (which would include the Visitor's or User's email address, IP address, and certain Intake Questionnaire responses).

45. But, as discussed in Paragraphs 46-57 below, these privacy policy representations misled Visitors and Users. In fact, Respondent used and disclosed Visitors' and Users' health information for advertising purposes, and Respondent disclosed this information to third parties for their own purposes, from 2013 to December 2020. Respondent used and disclosed this information for advertising purposes through various means, including by uploading consumers' email addresses to third-party advertising platforms and through web beacons (specifically pixels) Respondent had placed on various pages of the Multi-Sites.

### **B. Respondent Used and Disclosed Millions of Consumers' Health Information for Advertising**

46. Since 2013, Respondent has repeatedly broken each of its aforementioned privacy promises, using Visitors' and Users' email addresses, IP addresses, enrollment in the Service, and certain Intake Questionnaire responses for various advertising purposes, including (1) re-targeting Visitors with advertisements for the Service; (2) using Users' health information to find and target potential new Users with advertisements—on the basis that these potential new Users were likely to sign up for the Service because they shared traits with current Users; and (3) optimizing Respondent's advertisements, which involved targeting advertisements at individuals with attributes similar to those that had previously responded to Respondent's ads, such as new Users. Using this health information for advertising, Respondent has brought in hundreds of thousands of new Users, resulting in millions of dollars in additional revenue.

47. Respondent utilized a number of third-party advertising platforms, including Facebook, Snapchat, Criteo, and Pinterest, to carry out this advertising. To do so, Respondent disclosed Visitors' and Users' email addresses, IP addresses, enrollment in the Service, and certain Intake Questionnaire responses to these third parties, as detailed below.

48. As noted above, each such disclosure of even a Visitor's or User's email address constituted a disclosure of the Visitor's or User's health information. Specifically, because Respondent collected email addresses only from Visitors and Users 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 a Visitor's or User's email address implicitly identified the Visitor or User as one seeking and/or receiving mental health treatment via the Service.

49. Although Respondent "hashed" Visitors' and Users' email addresses (i.e., converted the email addresses into a sequence of letters and numbers through a cryptographic tool) before disclosing them to third parties, the hashing was not meant to conceal the Visitors' and Users' identities from Facebook or the other recipient third parties. Rather, the hashing was done merely to hide the email addresses from a bad actor in the event of a security breach. In fact, Respondent knew that third parties such as Facebook were able to, and in fact would, effectively undo the hashing and reveal the email addresses of those Visitors and Users with accounts on the respective third parties' platforms, which is how Facebook matched these email addresses with

Facebook user IDs. Indeed, Facebook's standard terms of service, to which Respondent agreed, explained that Facebook would use hashed email addresses it received from Respondent to match Visitors and Users with their Facebook user IDs for advertising purposes, among other things. Thus, Respondent knew that by sending these lists of Visitors' and Users' email addresses to third parties, it was telling these third parties which of their users were seeking or in therapy through the Service.

50. In addition, Respondent disclosed the Visitor's or User's IP address in conjunction with other data about their enrollment in the Service and/or their Intake Questionnaire responses to third parties. Each such disclosure similarly constituted a disclosure of the Visitor's or User's health information because it both identified the individual (via the IP address) and conveyed to the recipient third party that the Visitor or User was seeking and/or receiving mental health treatment via the Service (via his or her enrollment in the Service or answering the Intake Questionnaire).

51. **Health information shared with Facebook:** Respondent disclosed Visitors' and Users' health information to Facebook in two ways.

52. First, Respondent compiled lists of Visitors' and Users' email addresses, which it then uploaded to Facebook to match these individuals to their Facebook user accounts in order to target them and others like them with advertisements. Between 2017 and 2018, Respondent uploaded lists of over 7 million Visitors' and Users' email addresses to Facebook. Facebook matched over 4 million of these Visitors and Users with their Facebook user IDs, linking their use of the Service for mental health treatment with their Facebook accounts. Several examples are listed below:

- a. January 2017 – October 2018: Respondent uploaded over 170,000 Visitors' and Users' email addresses to Facebook, re-targeting these individuals and targeting potential new Users with advertisements for the Service.
- b. January 2018 – October 2018: Respondent uploaded over 15,000 Users' email addresses to Facebook to find and target new potential Users with advertisements for the Service.
- c. October 2017: Respondent uploaded 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.

53. Second, from 2013 to December 2020, Respondent shared Visitors' and Users' email addresses, IP addresses, and records known as "Events" with Facebook. These Events automatically tracked certain actions of each Visitor and User on the Multi-Sites, such as when they answered certain questions on the Intake Questionnaire in a certain way or when a Visitor enrolled in the Service to become a User. Respondent recorded and automatically disclosed these Events to Facebook through web beacons Respondent had placed on each of the Multi-Sites. Respondent disclosed Visitors' and Users' IP addresses, email addresses, and/or other persistent identifiers to Facebook alongside the Events so that Facebook could match the Events

information with the Visitors' and Users' Facebook accounts for advertising. Several examples are listed below:

- a. January 2018: Respondent disclosed to Facebook that over 70,000 Visitors 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: Respondent disclosed to Facebook over 1.5 million Visitors' and Users' previous therapy—gathered through their affirmative responses to the Intake Questionnaire question “Have you been in counseling or therapy before?”—to re-target the Visitors with advertisements and optimize Respondent's advertisements.
- c. October 2018 – November 2020: Respondent used and shared over 3.5 million Visitors' and Users' “good” or “fair” financial status—gathered through the Intake Questionnaire—with Facebook to optimize Respondent's advertisements and to find potential new Users and target them with advertisements.
- d. January – December 2020: Respondent shared with Facebook the fact that over 180,000 Visitors had become paying Users—through an Event denoting they had entered credit card information after completing the Intake Questionnaire—to optimize Respondent's advertisements and to find potential new Users and target them with advertisements.

54. Respondent labeled the Intake Questionnaire responses concerning prior therapy and financial status with anonymous Event titles before giving them to Facebook; however, in July 2018, the previously mentioned inexperienced and insufficiently trained Junior Marketing Analyst whom Respondent had put in charge of Facebook advertising revealed certain Events' true meaning to Facebook via the Facebook employee that serviced Respondent's advertising account. For example, though an affirmative response to the question “Have you been in counseling or therapy before?” was coded as “AddToWishlist,” the analyst revealed to Facebook that this event meant that the “user completes questionnaire marking they have been in therapy before,” thereby disclosing millions of Visitors' and Users' prior therapy to Facebook.

55. **Health information shared with other third parties:** In January 2019, Respondent disclosed to Snapchat the IP addresses and email addresses of approximately 5.6 million Visitors to re-target them with advertisements for the Service. From July 2018 to January 2019, Respondent disclosed the email addresses of over 70,000 Visitors—including Pride Counseling and Faithful Counseling Visitors—to Criteo in order to re-target them with advertisements. And, from August 2019 to September 2020, Respondent disclosed Visitors' email addresses to Pinterest for advertising.

56. **Additional use of health information for advertising:** From November 2017 to October 2020, Respondent used information concerning approximately 600,000 Pride Counseling Visitors' or Users' mental health statuses and their connection with the Visitors' and Users' LGBTQ identities to optimize future advertisements for the Service on Facebook. Respondent gathered this information through the Intake Questionnaire whenever a Pride

Counseling Visitor or User revealed that the Visitor's or User's "LGBTQ identity is contributing to your mental health concerns." Respondent used Facebook to identify characteristics and interests common among these Visitors and Users and then to target future advertisements for the Service on Facebook to individuals with similar characteristics and interests.

57. **Failure to limit third parties' use of health information:** In disclosing Visitors' and Users' health information to Facebook and other third parties, Respondent 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. For example, Facebook's Business Tools Terms, to which Respondent agreed, stated that it "may also use Event Data . . . for research and development purposes, and to . . . improve the Facebook Company Products." Similarly, Pinterest's Ad Data Terms provided: "We use Ad Data you give us for measuring ad effectiveness, ad delivery and reporting, improving safety and security on Pinterest, research and product development, and for other uses that you give us permission for." And Facebook has in fact used the Visitor and User information it received from Respondent for its own purposes, including improving its advertising products, tracking suspicious activity on its platforms, and research and development.

58. Further, though Respondent has deleted some of the Visitor and User information it disclosed to third parties from those third parties' advertising platforms, this deletion did not remove the information from those third parties' underlying databases.

### C. Respondent's Deceptive Statements Were Material to Consumers

59. Respondent's deceptive privacy assurances were material to consumers.

60. Visitors and Users want to keep their health information private. Indeed, a senior BetterHelp employee acknowledged at an investigational hearing conducted by FTC staff that consumers want "privacy in the context of therapy."

61. And Respondent acknowledges that this information is sensitive. In fact, Respondent's customer service representatives tell consumers that their "name, age, address, *email*, *medical history*, conversations between you and your counselor" are "PHI" or "Protected Health Information"<sup>2</sup> (emphasis added).

62. Following the February 2020 publication of news reports that Respondent was sharing consumers' health information with third parties, including Facebook, numerous Users contacted Respondent and voiced their anger about the disclosures. For example, one individual noted: "I learned that you sell yet more private information to Facebook. This is disgusting. This information makes clients easily identifiable and your platform takes 100% control of its dissemination. I have no ability to decide where that information is sent. Only you do." Another stated: "I have not given ANY consent to share my information with ANYONE. ESPECIALLY ads targeting my mental health 'weakness.'" And another called Respondent an "untrustworthy

---

<sup>2</sup> Protected Health Information is information that is considered sensitive and is protected by federal health privacy laws in certain contexts, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

company.” Other Users demanded the truth as to Respondent’s data-sharing practices, asking for assurances as to the privacy of their health information.

63. Respondent scripted the following false responses, which customer service representatives provided to Respondent’s customers: (1) “At BetterHelp, we are fully committed to protecting data and will not pass any P[ersonally] I[dentifiable] I[nformation] and/or P[rotected] H[ealth] I[nformation] to external entities including our third party partners;” and (2) “your P[rotected] H[ealth] I[nformation] and P[ersonally] I[dentifiable] I[nformation] is protected and not exposed” to Facebook.

64. Similarly, several health insurance and patient-advocacy companies representing tens of thousands of Users contacted Respondent, looking for assurance that Users’ health information had not been shared with any third parties. Senior BetterHelp employees answered each such inquiry with a variation on the same falsehood, claiming again and again that Respondent did not share any health information with any third parties.

#### **D. Respondent’s Deceptive HIPAA Seal**

65. From September 2013 to December 2020, Respondent displayed seals—in proximity to seals provided by third parties to Respondent—implying Respondent’s purported compliance with HIPAA. These seals are circled in red below:

September 2013 – December 2015:



January 2016 – December 2020:



66. By displaying the HIPAA seals on every page of the Multi-Sites, Respondent signaled to consumers that a government agency or other third party had reviewed Respondent’s privacy and information security practices and determined that they met HIPAA’s requirements. In addition, Respondent represented to consumers that it was in fact “HIPAA certified,” with its customer service representatives informing consumers that “[y]ou will also be able to see our HIPAA certification at the bottom of” our webpages.

67. However, no government agency or other third party reviewed Respondent's information practices for compliance with HIPAA, let alone determined that the practices met the requirements of HIPAA.

68. In addition, hundreds of Respondent's therapists are not subject to HIPAA and the identifiable health information of Users who engage with those therapists is therefore not protected by HIPAA. Further, Respondent does not even know which of its therapists are, or are not, subject to HIPAA, and it does not know which data are, or are not, protected by that law.

69. In December 2020, after receiving a Civil Investigative Demand from the Commission, Respondent removed the "HIPAA" seals from the Multi-Sites.

### **III. Respondent's Unfair Business Practices**

#### **A. Respondent's Unreasonable Privacy Practices**

70. From at least 2017 to at least 2021, Respondent has engaged in a number of practices that, individually or taken together, failed to safeguard Visitors' and Users' health information with respect to the collection, use, and disclosure of that information. Among other things, Respondent:

- 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 Visitors' and Users' affirmative express consent to collect, use, and disclose their health information for Respondent's 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 Visitors' and Users' health information for their own purposes, including but not limited to research and improvement of their own products, when Respondent did not provide Visitors and Users notice or obtain their consent for such uses.

71. As a result, Respondent repeatedly misrepresented its practices with respect to the collection, use, and disclosure of Visitors' and Users' health information (*see* Paragraphs 19-57, 62-64), and Respondent failed to provide consumers with sufficient notice or obtain their consent

as to these practices. Respondent disclosed these Visitors' and Users' health information to numerous third parties without authorization.

72. These misrepresentations went on for years because, until no earlier than January 2021, Respondent did nothing to ensure that its collection, use, and disclosure practices complied with their privacy promises to Visitors and Users. Indeed, neither the head of Respondent's marketing team, nor the analyst whom Respondent put in charge of advertising on Facebook reviewed the privacy policy on a regular basis, and there was no company requirement that anyone on the marketing team review the policy until no earlier than January 2021.

## **B. Injury to Consumers**

73. Respondent's collection, use, and disclosure of millions of Visitors' and Users' health information without reasonable privacy practices or safeguards has caused or is likely to cause them substantial injury. This health information—including whether Visitors and Users have previously been in therapy, the fact that they are seeking therapy or in therapy via the Service, and whether their LGBTQ status is affecting their mental health, together with identifying information such as their email addresses and IP addresses—is highly sensitive. Disclosure of this information without these Visitors' and Users' authorization is likely to cause them stigma, embarrassment, and/or emotional distress. Exposure of this information may also affect these Visitors' and Users' ability to obtain and/or retain employment, housing, health insurance, or disability insurance.

74. 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 Respondent's deceptive privacy assurances. Had Respondent 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, Respondent'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 Respondent's services. Consumers have therefore been injured by having to pay this price premium.

75. These harms were not reasonably avoidable by consumers. It was effectively impossible for Visitors and Users to know that Respondent was using and disclosing their health information for advertising purposes because Respondent actively concealed the practices through repeated misrepresentations and a lack of notice. Indeed, as described in Paragraph 62, numerous Users expressed outrage about the disclosures upon learning of them.

76. These harms were not outweighed by countervailing benefits to consumers or competition. Indeed, Respondent compromised consumers' health information for Respondent's own financial benefit through the growth of its user base, which only compounded these injuries by subjecting more Visitors and Users to Respondent's deceptive and unfair practices.

**Count I**  
**Unfairness – Unfair Privacy Practices**

77. As described in Paragraphs 16-17 and 70-72, Respondent failed to employ reasonable measures to protect consumers' health information in connection with the collection, use, and disclosure of that information, resulting in the improper and unauthorized disclosure of that information to numerous third parties for advertising and other purposes.

78. Respondent's acts or practices as set forth in Paragraph 77 caused or are likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves, as described in Paragraphs 73-76.

79. Therefore, Respondent's acts or practices as set forth in Paragraphs 77-78 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

**Count II**  
**Unfairness – Failure to Obtain Affirmative Express Consent  
Before Collecting, Using, and Disclosing Consumers' Health Information**

80. As described in Paragraphs 19-58, Respondent failed to obtain consumers' affirmative express consent before collecting, using, and disclosing to third parties those consumers' health information.

81. Respondent's acts or practices as set forth in Paragraph 80 caused or are likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves, as described in Paragraphs 73-76.

82. Therefore, Respondent's acts or practices as set forth in Paragraphs 80-81 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

**Count III**  
**Failure to Disclose – Disclosure of Health Information for Advertising and Third Parties'  
Own Uses**

83. As described in Paragraphs 41 and 44, Respondent represented, directly or indirectly, expressly or by implication, that it would disclose consumers' health information to third parties for limited purposes, and the listed purposes did not include advertising or third parties' own uses.

84. In making the representations described in Paragraph 83, Respondent failed to disclose, or failed to disclose adequately to consumers, that it disclosed consumers' health information to third parties, including Facebook, Pinterest, Snapchat, and Criteo, for advertising as well as third parties' own uses, as alleged in Paragraphs 47-57. This additional information would have been material to consumers in their decisions to use Respondent's services.

85. Therefore, Respondent's acts or practices as set forth in Paragraphs 83-84 constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

#### **Count IV**

##### **Failure to Disclose – Use of Health Information for Advertising**

86. As described in Paragraphs 41 and 44, Respondent represented, directly or indirectly, expressly or by implication, that it would use consumers' health information for limited purposes, and the listed purposes did not include advertising or advertising-related purposes.

87. In making the representations described in Paragraph 86, Respondent failed to disclose, or failed to disclose adequately to consumers, that it used consumers' health information for advertising and advertising-related purposes, as alleged in Paragraphs 46, 53, and 56. This additional information would have been material to consumers in their decisions to use Respondent's services.

88. Therefore, Respondent's acts or practices as set forth in Paragraphs 86-87 constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

#### **Count V**

##### **Privacy Misrepresentation – Disclosure of Health Information for Advertising and Third Parties' Own Uses**

89. As described in Paragraphs 28-31, 42-43, and 63-64, Respondent represented, directly or indirectly, expressly or by implication, that it would not disclose consumers' health information to any third party for advertising or that third party's own uses.

90. In fact, as set forth in Paragraphs 46-55 and 57, Respondent disclosed consumers' health information to third parties, including Facebook, Pinterest, Snapchat, and Criteo, for advertising and those third parties' own uses. Therefore, the representations set forth in Paragraph 89 are false or misleading.

91. Therefore, Respondent's acts or practices as set forth in Paragraphs 89-90 constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

#### **Count VI**

##### **Privacy Misrepresentation – Use of Health Information for Advertising**

92. As described in Paragraph 42, Respondent represented, directly or indirectly, expressly or by implication, that it would not use consumers' health information for advertising or advertising-related purposes.

93. In fact, as set forth in Paragraphs 46, 53, and 56, Respondent did use consumers' health information for advertising and advertising-related purposes. Therefore, the representations set forth in Paragraph 92 are false or misleading.

94. Therefore, Respondent's acts or practices as set forth in Paragraphs 92-93 constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

**Count VII**  
**Privacy Misrepresentation – Disclosure of Health Information**

95. As described in Paragraphs 23-26, Respondent represented, directly or indirectly, expressly or by implication, that it would not disclose consumers' health information to anyone except each consumer's licensed therapist.

96. In fact, as set forth in Paragraph 46-54, Respondent disclosed consumers' health information to at least one entity other than each consumer's licensed therapist—Facebook. Therefore, the representations set forth in Paragraph 95 are false or misleading.

97. Therefore, Respondent's acts or practices as set forth in Paragraphs 95-96 constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

**Count VIII**  
**Privacy Misrepresentation – HIPAA Certification**

98. As described in Paragraphs 65-66, Respondent represented, expressly or by implication, directly or indirectly, that a government agency or other third party had reviewed Respondent's privacy and information practices and determined that they met HIPAA's requirements.

99. In fact, as set forth in Paragraphs 67-68, no government agency or other third party had ever reviewed Respondent's privacy or information security practices and determined that they met HIPAA's requirements.

100. Therefore, Respondent's acts or practices as set forth in Paragraphs 98-99 constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this \_\_\_\_ day of \_\_\_\_\_ 2022, has issued this complaint against Respondent.

By the Commission.

April J. Tabor  
Secretary

SEAL:

**Analysis of Proposed Consent Order to Aid Public Comment**  
***In the Matter of BetterHelp, Inc.***  
**File No. 2023169**

The Federal Trade Commission (the “Commission”) has accepted, subject to final approval, an agreement containing a consent order from BetterHelp, Inc. (“Respondent” or “BetterHelp”).

The proposed consent order (“Proposed Order”) has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement, along with any comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the Proposed Order.

BetterHelp is an online mental-health counseling service that matches consumers with one of BetterHelp’s over 25,000 contracted licensed therapists. Through BetterHelp’s websites and apps, consumers can communicate with therapists via video conferencing, text messaging, live chat, and audio calls. BetterHelp has offered this service under several names, including BetterHelp Counseling, Faithful Counseling, Pride Counseling, ReGain, Terapeuta, iCounseling, and MyTherapist.

To sign up for BetterHelp’s counseling service, a consumer must complete an online intake questionnaire, answering detailed questions about the consumer’s mental health status and history (the “Intake Questionnaire”). Following completion of the Intake Questionnaire, the consumer can create an account by providing the consumer’s name or nickname, email address, phone number, and emergency contact information.

As consumers progressed through the Intake Questionnaire, BetterHelp represented that the consumers’ information “will stay private between you and your counselor.” Similarly, when a consumer completed the Intake Questionnaire and signed up for an account to use Faithful Counseling, Pride Counseling, or Teen Counseling, BetterHelp represented that the consumer’s email address would be “kept strictly private” and “never shared, sold or disclosed to anyone.” BetterHelp made additional privacy guarantees in its privacy policies—first implicitly and then explicitly—of limited use and limited disclosure of consumers’ email addresses, IP addresses, and health information. Despite representing to consumers that BetterHelp would keep consumers’ information private and only use their information for non-advertising purposes, BetterHelp used and disclosed information obtained from consumers through the Intake Questionnaire and sign-up process for advertising.

Additionally, BetterHelp prominently displayed a seal—in close proximity to several other seals provided by third parties—that attested to BetterHelp’s purported compliance with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), a statute that sets forth privacy and information security protections for health information. In addition, BetterHelp represented to consumers that it was in fact

“HIPAA certified,” with its customer service representatives informing consumers that “[y]ou will also be able to see our HIPAA certification at the bottom of” our webpages. However, no government agency or other third party had reviewed BetterHelp’s information practices for compliance with HIPAA, let alone determined that the practices met the requirements of HIPAA.

The Commission’s proposed eight-count complaint alleges that BetterHelp violated Section 5(a) of the Federal Trade Commission Act by: (1) unfairly failing to employ reasonable measures to protect consumers’ health information in connection with the collection, use, and disclosure of that information (Count I); (2) unfairly failing to obtain consumers’ affirmative express consent prior to collecting, using, and disclosing consumers’ health information (Count II); (3) failing to disclose that it shared consumers’ health information with third parties for BetterHelp’s advertising purposes and the recipient third parties’ own business purposes, and failing to disclose that BetterHelp used consumers’ health information to target the consumers and others with advertisements (Counts III and IV); (4) misrepresenting that it would not disclose consumers’ health information to third parties for advertising and the recipient third parties’ own business purposes, that it would not use such information for advertising or advertising-related purposes, and that it would not share such information with anyone except each consumer’s licensed therapist (Counts V-VII); and (5) misrepresenting that a governmental agency or third party had reviewed BetterHelp’s practices and determined that such practices met the requirements of HIPAA (Count VIII).

### **Summary of Proposed Order with BetterHelp**

The Proposed Order contains provisions designed to prevent BetterHelp from engaging in the same or similar acts or practices in the future.

**Part I** of the Proposed Order prohibits BetterHelp from sharing individually identifiable information relating to the past, present, or future physical or mental health or condition(s) of a consumer with any Third Party (i.e., any party other than BetterHelp, its service providers, therapists or counselors employed by or contracted with BetterHelp, certain employee benefit programs, and entities using consumers’ information for other very limited purposes) for advertising. Part I also prohibits BetterHelp from sharing consumers’ personal information more generally with Third Parties for the purpose of re-targeting (i.e., sharing personal information of consumers who have previously engaged with BetterHelp, such as by visiting one of its websites or using one of its apps, to send advertisements to those consumers).

**Part II** of the Proposed Order requires that, before it can share a consumers’ personal information with a Third Party for any purpose that is not prohibited under Part I, BetterHelp must obtain that consumer’s affirmative express consent, which includes informing the consumer of the information to be disclosed, the third parties that will receive the information, and how the information will be used.

**Part III** of the Proposed Order prohibits BetterHelp from misrepresenting: (1) the extent to which it collects, maintains, uses, discloses, deletes, or permits or denies access

to any Covered Information, or the extent to which it protects the privacy, security, availability, confidentiality, or integrity of Covered Information; (2) the purposes for which BetterHelp or any entity to whom it discloses or permits access to Covered Information collects, maintains, uses, discloses, or permits access to such information; (3) the extent to which a consumer can maintain privacy and anonymity when visiting or using BetterHelp's online properties; (4) the extent to which consumers may exercise control over BetterHelp's collection of, maintenance of, use of, deletion of, disclosure of, or permission of access to Covered Information; (5) the extent to which BetterHelp is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security or any other compliance program sponsored by a government or any self-regulatory or standard-setting organization; and (6) the extent to which BetterHelp is covered by HIPAA, and the extent that its privacy and information practices are in compliance with HIPAA requirements.

**Part IV** of the Proposed Order requires BetterHelp to identify to the Commission which Third Parties received consumers' personal information from BetterHelp without their consent and what personal information each such Third Party received. Part IV also requires that BetterHelp then ask those Third Parties to delete such personal information.

**Part V** of the Proposed Order requires that BetterHelp provide notice to consumers who created an account with BetterHelp prior to January 1, 2021, that BetterHelp may have used and disclosed their personal information for advertising.

**Part VI** of the Proposed Order requires BetterHelp to establish and implement, and thereafter maintain, a comprehensive privacy program that protects the privacy, security, availability, confidentiality, and integrity of consumers' Covered Information.

**Part VII** of the Proposed Order requires BetterHelp to obtain initial and biennial privacy assessments by an independent, third-party professional ("Assessor") for 20 years, and **Part VIII** requires BetterHelp to cooperate with the Assessor in connection with the assessments required by Part VII.

**Part IX** of the Proposed Order requires that a BetterHelp executive certify the company's compliance with the Proposed Order.

**Part X** of the Proposed Order requires BetterHelp to notify the Commission following the discovery of a violation of Parts I, II, or III of the Proposed Order.

**Part XI** of the Proposed Order requires BetterHelp to pay \$7,800,000 in monetary relief for consumer redress, and **Part XII** describes the procedures and legal rights related to that payment.

**Part XIII** of the Proposed Order requires BetterHelp to provide information to, and pay for, an independent redress administrator ("Administrator") selected by the Commission, which will be responsible for administration of consumer redress.

**Parts XIV through XVII** of the Proposed Order are reporting and compliance

provisions, which include recordkeeping requirements and provisions requiring BetterHelp to provide information or documents necessary for the Commission to monitor compliance.

**Part XVIII** states that the Proposed Order will remain in effect for twenty (20) years, with certain exceptions.

The purpose of this analysis is to aid public comment on the Proposed Order. It is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify in any way the Proposed Order's terms.