UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

UNITED STATES OF AMERICA, **Plaintiff,** **v.** **CEREBRAL, INC., a corporation, and KYLE ROBERTSON, individually,** **Defendants.**	**Case No. _____** **JURY TRIAL DEMANDED**

THE UNITED STATES' COMPLAINT FOR PERMANENT INJUNCTION, MONETARY RELIEF, CIVIL PENALTIES, AND OTHER RELIEF

Plaintiff, the United States of America, upon referral from the Federal Trade Commission, for its Complaint alleges:

1. Plaintiff brings this action under Sections 5(m)(1)(A), 13(b), 16(a), and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(m)(1)(A), 53(b), 56(a), 57b; Section 8023 of the Opioid Addiction Recovery Fraud Prevention Act of 2018 ("Opioid Act"), 15 U.S.C. § 45d; and Section 5 of the Restore Online Shoppers' Confidence Act ("ROSCA"), 15 U.S.C. § 8404, which authorize Plaintiff to seek, and the Court to order, permanent injunctive relief, monetary relief, civil penalties, and other relief for Defendants' acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a); Section 8023 of the Opioid Act, 15 U.S.C. § 45d; and Section 4 of ROSCA, 15 U.S.C. § 8403. Defendants' violations concern deceptive and unfair privacy and data security practices, failures to clearly and accurately disclose material terms related to data privacy, data security, and cancellation, failures to obtain

consumers' express informed consent relating to those material terms, and failures to provide a simple mechanism to stop recurring charges in connection with the promotion or offering for sale of online health care services, such as mental health treatment, medication management, and substance use disorder treatment services.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), 1345, and 1355.

3. Venue is proper in this district under 28 U.S.C. § 1391(b)(2), (b)(3), (c)(2), and (d), 1395(a), and 15 U.S.C. § 53(b).

THE PARTIES

4. Plaintiff is the United States of America.

5. Defendant Cerebral, Inc. ("Cerebral"), is a Delaware corporation that does business remotely or through virtual offices, and has a principal address at 2093 Philadelphia Pike #9898, Claymont, Delaware 19703. Cerebral transacts or has transacted business in this District and throughout the United States.

6. Defendant Kyle Robertson ("Robertson") resides, and at times relevant to this Complaint resided, in this District. He served as Chief Executive Officer of Cerebral from at least October 2019 to May 2022. At times relevant to this Complaint, acting alone or in concert with others, Robertson formulated, directed, controlled, had the authority to control, or participated in the acts and practices of Cerebral, including acts and practices set forth in this Complaint.

7. Robertson led a wide array of Cerebral subject matter areas pertinent to this case. His leadership of Cerebral extended to serving as the designated reviewer and approver of several important company policies, including policies relevant to this case such as those related to privacy, disclosure of user data, data security, data breaches, and Health Insurance Portability and Accountability Act ("HIPAA").

8. In addition to setting key policies, Robertson was closely involved in many facets of Cerebral's day-to-day operations and was responsible for "defining strategy" for its operations. Robertson helped to develop Cerebral's compliance and data security functions and supervised direct reports who evaluated and managed the company's data security practices. Robertson also supervised Cerebral's marketing team, provided detailed feedback and approval for Cerebral's advertisements, received information security or risk management briefings from Cerebral's Head of Engineering or Chief Information Security Officer and served as a member of Cerebral's Data Breach Response Team in a reporting and approval capacity.

9. Robertson, in connection with the matters alleged in this Complaint, transacts or has transacted business in this District and throughout the United States.

COMMERCE

10. At all times relevant to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

THE FTC ACT

11. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

12. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5 of the FTC Act.

13. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

THE OPIOID ACT

14. Section 8023 of the Opioid Act, 15 U.S.C § 45d, prohibits any "unfair or deceptive act or practice with respect to any substance use disorder treatment service." 15 U.S.C. § 45d(a). Section 8022 of the Opioid Act defines "substance use disorder treatment service" as "a service that purports to provide referrals to treatment, treatment, or recovery housing for people diagnosed with, having, or purporting to have a substance use disorder, including an opioid use disorder." Pub. L. No. 115-271 § 8022.

15. Pursuant to the Opioid Act, a violation of 15 U.S.C. § 45d(a) shall be treated as a violation of a rule promulgated under Section 18 of the FTC Act, 15 U.S.C. § 57a. 15 U.S.C. § 45d(b)(1). Section 19b(b) of the FTC Act, 15 U.S.C. § 57b(b), authorizes this Court to award such relief as it finds necessary to redress injury to consumers resulting from each Opioid Act violation, including but not limited to monetary relief. Section 5(m)(1)(A) of the FTC Act, 15

U.S.C. § 45(m)(1)(A), authorizes this Court to award civil penalties for each violation of the Opioid Act.

THE RESTORE ONLINE SHOPPERS' CONFIDENCE ACT

16. In 2010, Congress passed the Restore Online Shoppers' Confidence Act, 15 U.S.C. §§ 8401 *et seq.* In passing ROSCA, Congress declared that "[c]onsumer confidence is essential to the growth of online commerce. To continue its development as a marketplace, the Internet must provide consumers with clear, accurate information and give sellers an opportunity to fairly compete with one another for consumers' business." Section 2 of ROSCA, 15 U.S.C. § 8401.

17. ROSCA prohibits the sale of goods or services on the Internet through negative option marketing without meeting certain requirements to protect consumers. Section 4 of ROSCA, 15 U.S.C. § 8403, prohibits charging consumers for goods or services sold in transactions effected on the Internet through a negative option feature, as that term is defined in the Federal Trade Commission's ("FTC")'s Telemarketing Sales Rule ("TSR"), 16 C.F.R. § 310.2(w), unless the seller, among other things, clearly and conspicuously discloses all material terms of the transaction before obtaining the consumer's billing information, obtains a consumer's express informed consent before charging the consumer's credit card, and provides a simple mechanism for a consumer to stop recurring charges. 15 U.S.C. § 8403.

18. The TSR defines a negative option feature as a provision in an offer or agreement to sell or provide any goods or services "under which the client's silence or failure to take an

affirmative action to reject goods or services or to cancel the agreement is interpreted by the seller as acceptance of the offer." 16 C.F.R. § 310.2(u).

19. ROSCA is considered an FTC Rule under Section 18 of the FTC Act, 15 U.S.C. § 57a. Therefore, a Court can impose a civil penalty "of not more than [$51,744] for each violation" of ROSCA where a defendant acted "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule." *Id.* § 45(m)(1)(A); 16 C.F.R. § 1.98(d) (adjusting the penalty cap for inflation). Moreover, under Section 19b(b) of the FTC Act, 15 U.S.C. § 57b(b), this Court may award such relief as it finds necessary to redress injury to consumers resulting from each ROSCA violation, including but not limited to monetary relief.

DEFENDANTS' BUSINESS ACTIVITIES

I. Cerebral's Business Activities

20. Since October 2019, Cerebral has promoted or sold subscription services offering online health care treatment or "telehealth," including mental health treatment and/or medication management services, through websites and mobile apps to hundreds of thousands of patients struggling with depression, anxiety, and other issues, including, in at least 2021 and 2022, substance use disorders such as opioid use disorder and alcohol use disorder for thousands of patients. It has reportedly raised several hundreds of millions of dollars and been valued at $4.8 billion.

21. Cerebral matches its subscribers with treatment providers and furnishes them access to providers, who provide virtual treatment and are employed by or are independent

contractors of its corporate affiliates, including Cerebral Medical Group, P.A., and Cerebral Medical Group, P.C. (collectively, "Cerebral Medical Groups," "Group," "CMG," or "CMGs").

22. Cerebral has promoted or sold its subscription services on a negative option basis. A negative option is an offer in which the seller treats a consumer's silence (*i.e.,* the failure to reject an offer or cancel an agreement) as consent to be charged for goods or services. Cerebral has charged clients on a recurring basis for subscriptions that automatically renew monthly unless clients successfully cancel before the end of their monthly billing cycles.

23. In its operations, Cerebral has routinely collected and stored sensitive personal health information ("PHI") and other sensitive information of consumers seeking treatment. This information includes full names; home and email addresses; phone numbers; birthdates; IP addresses; audio, images, and videos of clients; medical and prescription histories; other specific health information, including treatment plans and treatment appointment dates; pharmacy and health insurance information; religious affiliations and beliefs; political affiliations and beliefs; sexual orientation; Social Security, payment account, and driver's license numbers; and information relating to criminal background checks.

24. In urging patients to disclose sensitive PHI and sign up for Cerebral's services, Defendants have disseminated or caused to be disseminated privacy and data security assurances to consumers, pledging, for example, "[c]onfidential treatment from the privacy of your home" that is "private, secure, and non-judgmental," "safe, secure, and discreet," or "use[s] the latest information security technology to protect your data."

25. As detailed herein, however, at least during Robertson's tenure as its Chief

Executive Officer, Cerebral: (a) misrepresented the extent to which and the purposes for which Cerebral would use and disclose at least hundreds of thousands of patients' personal information, as well as its safeguards against unauthorized disclosure of such information; (b) mishandled and exposed hundreds of thousands of patients' personal information; and (c) failed to provide patients with a simple means to cancel their subscriptions and stop recurring charges. Instead, to deter people from cancelling, Defendants deliberately made the cancellation process burdensome and challenging, while taking millions of dollars from vulnerable consumers, including patients suffering from mental health problems, for subscriptions after they had asked it to cancel those subscriptions.

II. Robertson's Leadership, and Extensive Personal Involvement in Several Major Facets, of Cerebral

26. Robertson co-founded Cerebral in 2019. Until being terminated from the company in May 2022, he served as its Chief Executive Officer. Through his singularly powerful position, and by virtue of the close control he exercised over Cerebral's relevant teams, operations, and policies, Robertson contributed extensively and directly to the chronic misconduct alleged herein.

27. In its first year, Cerebral was a small start-up with a limited number of employees working under Robertson's supervision. While Cerebral grew substantially over the next few years, until his departure, Robertson continued to control several major operational and strategic facets of the company.

28. As CEO, Robertson helped develop and control many of Cerebral's core functions. For instance, in 2019, Robertson led a wide array of Cerebral subject matter areas,

including Legal & Regulatory. He discussed with Cerebral's legal and compliance personnel its legal and regulatory issues pertaining to data privacy, data security, breaches, and cancellation and refund processes. Robertson was so attuned to the application of relevant statutes to Cerebral's practices that he provided legal guidance in response to employees' questions about whether company practices met legal requirements. Similarly, Robertson participated directly in shaping the company's strategy and statements in dealing with regulators in the aftermath of data breaches.

29. Robertson also closely supervised Cerebral's Growth Team, which facilitated the company's aggressive marketing and advertising strategy.

30. Robertson's leadership of Cerebral extended to serving as the designated reviewer and approver of several cornerstone company policies, including policies concerning privacy, disclosure of user data, data security, data breaches, and HIPAA. Robertson personally approved these policies. For example, he approved the following Cerebral policies: Cerebral's original policy on the "Use/Disclosure of Protected Health Information for Marketing Purposes" (stressing that "Cerebral will obtain an authorization for any use or disclosure of PHI [Personal Health Information] for marketing…"); Cerebral's original "HIPAA Privacy Program Implementation & Oversight" and "HIPAA Security Oversight" policies (detailing proper standards for safeguarding electronic PHI); Cerebral's original "Right to Notice" policy requiring clear, upfront disclosure to users of all "uses and disclosures" that their PHI may be used for, and requiring authorization for any uses or disclosures relating to "marketing, and the sale of protected health information"; Cerebral's original "Validation of Content of a Patient

Authorization" policy, outlining the criteria for a sufficient "patient authorization for use or disclosure of [PHI]"; Cerebral's "Notice of Health Plan Privacy Practices" policy, explaining to patients how their medical information "may be used and disclosed"; and Cerebral's original "Security Incident Response Policy," outlining protocols that would be followed in instances of data security breaches.

31. In addition to setting key policies, Robertson was closely involved in many aspects of Cerebral's day-to-day operations. Cerebral's teams of product managers, engineers, marketers, and compliance personnel liaised closely with Robertson and frequently required his approval for key strategic and operational decisions.

32. Robertson also helped to develop Cerebral's compliance and data security functions. At relevant times, Cerebral's Chief Integrity and Compliance Officer and Cerebral's Vice President of Product and Engineering reported directly to Robertson. They regularly briefed him on data privacy and data security issues and solicited his guidance on relevant company practices and strategy.

33. Robertson regularly reviewed and approved Cerebral's decisions to disclose patient data to third parties, and to use third-party software applications for storing and transmitting confidential user data.

34. Robertson also played a key role in shaping and approving Cerebral's annual budgets, which invested disproportionately in growth and marketing efforts while simultaneously deprioritizing Cerebral's compliance and data security functions.

III. Defendants' Unlawful Privacy and Data Security Practices

35. Defendants have made or have caused to be made numerous misrepresentations and omissions regarding Cerebral's privacy and data security practices to encourage consumers to disclose their sensitive PHI and subscribe to Cerebral's services. Consumers have relied on these representations or omissions and have been misled as a result.

A. Defendants' Privacy and Data Security Assurances to Consumers

36. In connection with the promotion and sale of Cerebral's services, Defendants have disseminated, or caused to be disseminated, assurances about the privacy or security of sensitive PHI that consumers entrust to Cerebral. These assurances have touted Cerebral's purported restrictions on the use and disclosure of consumers' sensitive data, as well as its purported safeguards against unauthorized disclosure of such data.

1. Assurances in Cerebral's Promotional Claims

37. For example, Cerebral's "How it works" screen has touted the privacy and security of its services, stating: "Come as you are, without even having to leave home. We're tearing down the walls of mental health stigma, but you're more than welcome to receive your care from the comfort of your own home. It's private, secure, and non-judgmental."

38. In an online blog post titled, "What to know about getting antidepressants online with telehealth," Cerebral has represented (bold emphasis in original, italics added):

> • ***Keep things private and confidential***
> With telehealth, care is right at your fingertips and at your discretion. Have your meetings at work or at home while taking care of your kids. Remote healthcare fits into your schedule, wherever you are.
> . . . .
> Ultimately, remote depression and anxiety treatment is safe, *secure, and discreet*.

. . . .

> Seeking treatment for your depression and anxiety is simple and *secure*. If you feel like you might be experiencing symptoms of depression, we hope you'll consider taking our free emotional assessment [hyperlinked] to determine if treatment is right for you.

39. In other materials displayed on its websites and/or apps, Cerebral has promised its subscribers can expect "Confidential treatment from the privacy of your home" or "discreet, judgment-free . . . screening and treatment," among similar claims.

40. Additionally, since at least September 2022, Cerebral's "Our Promise to Our Patients" screen has stated (bold emphasis in original):

> **Our Promise to Our Patients**
> At Cerebral, **patients come first.**
> . . . .
> **How do we ensure the highest quality of care?**
> We follow a clinical code of ethics, derived from the Institute of Medicine's Six Domains of Clinical Quality, as guiding principles for care. We deliver care that is:
> . . . .
> **Secure**
> We use the latest information security technology to protect your data, which is not shared without your consent, and will only be used internally to improve clinical care.

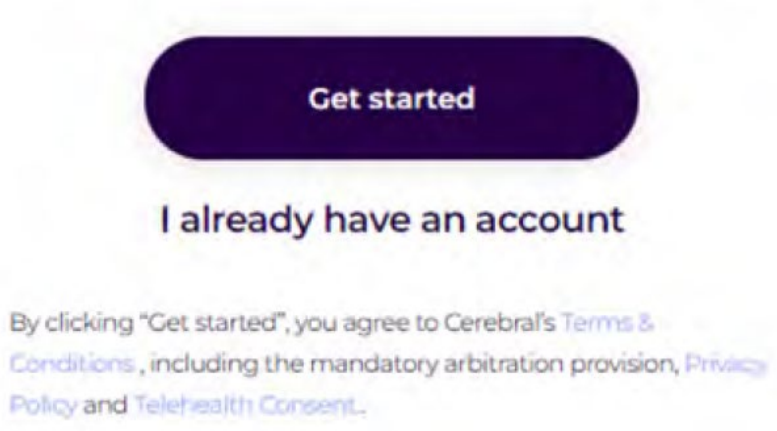
2. Assurances in Cerebral's Online Enrollment Path

41. Cerebral's enrollment path has reinforced these assurances and referenced its Privacy Policy.

42. To enroll consumers in one or more of its subscription services and subsequently charge them, Cerebral has required consumers visiting its websites or apps to create an account, providing personal information such as their name, phone number, email address, birthdate, and their interest in obtaining mental health treatment. Thereafter, in many instances, Cerebral has

required consumers to complete an online assessment to answer detailed questions about themselves and their mental health, and then select a treatment plan. In performing these steps, consumers gave Cerebral sensitive PHI such as that described above.

43. In many instances, Cerebral also has required consumers beginning its intake assessment to click on a large button labeled, "Get started." Beneath this button, and under large bold text, smaller non-bolded text has appeared. The text below the button asserted that by clicking the "Get started" button, consumers agree to Cerebral's terms and conditions, which include an arbitration provision, a Privacy Policy, and a Telehealth Consent.



44. However, this screen did not provide information about the specific information practices to which Cerebral asked consumers to agree. Instead, it merely provided hyperlinks to Cerebral's terms and its Privacy Policy and Telehealth Consent.

45. Cerebral has at times provided a hyperlink to its Privacy Policy on other screens; however, this link typically has appeared in small print, at the bottom of the screens, often lodged between links to its terms and conditions and a website sitemap, and surrounded by other links, such as links to various social media channels, and/or other visual elements or depictions.

46. In many instances, Cerebral's screens asking consumers to select a treatment plan have contained text echoing its other privacy and data security assurances (*e.g.*, "Chat securely with your therapist anytime") – such text appearing more than once on the screen in some instances.

47. After consumers select treatment plans, in many instances, Cerebral has presented a final checkout screen displaying features of the selected plan, its price, blanks for consumers to provide promotional codes as well as their payment information, and a "Submit" button with small print appearing below it. Until May 2022, in numerous instances, that small print asserted that by clicking the "Submit" button, consumers consented to Cerebral's payment terms and recurring billing policy. The small print did not reference its Privacy Policy or its privacy or data security assurances. Starting in May 2022, in numerous instances, the small print asserted that by clicking the "Submit" button, consumers agreed to Cerebral's terms and Privacy Policy, among other things. As before, the screen did not display the referenced terms and Privacy Policy.

3. Assurances in Cerebral's Privacy Policy and Other Documents Published Online

48. Prior to December 2020, Cerebral's original Privacy Policy, which was over seven single-spaced pages in length, contained text five pages in asserting that Cerebral could disclose consumers' personal information to third party service providers for purposes of data analysis as well as other purposes. However, the Privacy Policy also asserted, seven pages in, that Cerebral "agreed that its collection, use, and disclosure of your [protected health

information][1] on behalf of your physician or health care provider will be done consistent with the Notice of Privacy Practices" of its affiliated Cerebral Medical Group.

49. Until May 2022, the Notice of Privacy Practices published on Cerebral's websites provided (emphasis added):

> *Without your authorization, we are expressly prohibited from using or disclosing your protected health information for marketing purposes.* We may not sell your protected health information without your authorization.

50. Between 2020 and May 2022, Cerebral's Privacy Policy also asserted, several pages in, that Cerebral "may also collect data by using 'pixel tags,' 'web beacons,' 'clear GIFs,' or similar means . . . that allow us to know when you visit our [w]ebsites or [a]pps. Through pixel tags, we obtain *non-personal information or aggregate information* that can be used to enhance your online experience and understand traffic patterns." (emphasis added).

51. In December 2020, Cerebral's Privacy Policy ballooned to fifteen single-spaced pages, and Cerebral added a statement five pages in, admitting for the first time that it used Facebook Pixel, a web analytics and advertising service by Facebook, Inc. ("Facebook") that "uses cookies, pixel tags, and other storage and tracking technology to collect or receive information from [Cerebral's] [w]ebsites and [a]pps based on [consumers'] usage activity." In this inconspicuous statement, Cerebral stated, "Facebook can connect this data with your

[1] Defendants' Privacy Policy has defined "protected health information" to include health information protected under the Health Insurance Portability and Accountability Act ("HIPAA"), and the Notice of Privacy Practices of its affiliated Cerebral Medical Group has defined "protected health information" to mean "information about you, including demographic information, that may identify you and that relates to your past, present or future physical health or condition, treatment or payment for health care services."

Facebook account and use it for its own and others[’] advertising purposes.” Further, Cerebral added another inconspicuous statement disclosing for the first time its use of Google Analytics and third-party cookies deployed on its websites by three other third party firms.

52. Notwithstanding these statements, Cerebral’s Privacy Policy and the Notice of Privacy Practices also have purported to further limit Cerebral’s use and disclosure of consumers’ sensitive PHI. For example, in 2020 and 2021, Cerebral’s Privacy Policy stated:

> Cerebral will use or disclose PHI [(protected health information)] only as permitted in Cerebral’s agreements with CMG (or your own medical provider if you do not use a CMG Provider) and we only collect the PHI we need to fully perform our services and to respond to you or your Provider. We may use your PHI to contact you to the extent permitted by law, to provide requested services, to provide information to your Providers and insurers, to obtain payments for our services, to respond to your inquiries and requests, and to respond to inquiries and requests from your Providers and benefits program. We may combine your information with other information about you that is available to use, including information from other sources, such as from your Providers, insurers or benefits program, in order to maintain an accurate record of our participants. *PHI will not be used for any other purpose, including marketing, without your consent.*

(emphasis added). Similar text also appeared in Cerebral’s Privacy Policy in 2022.

53. Further, the “Telehealth Informed Consent” screen on Cerebral’s websites or apps contained additional assurances to consumers concerning privacy and data security:

> The electronic communication systems we use will incorporate network and software security protocols to protect the confidentiality of patient identification and imaging data and will include measures to safeguard the data and to ensure its integrity against intentional or unintentional corruption. All the services delivered to the patient through telehealth will be delivered over a secure connection that complies with the requirements of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).
> . . . .
> In very rare events, security protocols could fail, causing a breach of privacy of personal medical information.
> . . . .

> Federal and state law requires health care providers to protect the privacy and the security of health information. I am entitled to all confidentiality protections under applicable federal and state laws.

B. Defendants' Deceptive and Unlawful Privacy Practices

1. Contrary to These Repeated Assurances, Defendants Have Used and Disclosed Hundreds of Thousands of Patients' Sensitive PHI for Marketing Purposes

54. Since the inception of Cerebral's advertising and marketing, Defendants have repeatedly broken their privacy assurances to hundreds of thousands of consumers by sharing, or allowing the sharing of, consumer information with numerous third parties whose services it has utilized to promote Cerebral's services.

55. For example, between 2019 and 2023, directly and indirectly, Defendants provided consumers' sensitive personal information to third parties for Cerebral's marketing purposes by using or integrating third party tracking tools into Cerebral's websites and apps, or allowing them to be used. These tracking tools (including tracking "pixels") collected and sent Cerebral's patients' PHI to third parties. Those third parties then used that PHI to provide advertising, data analytics, or other services to Cerebral. The data that Cerebral sent included consumers' contact information, persistent identifiers, and information about consumers' activities while using Cerebral's websites and/or apps. It also included medical or mental health information that was disclosed by users when they filled out Cerebral's mental health questionnaire or engaged with its website in ways that demonstrated interests in particular services and treatments.

56. Robertson helped direct the 2019 decision to deploy and use this technology.

Indeed, in blatant violation of several policies that he had reviewed and approved requiring Cerebral to obtain patients' consent to use their PHI, Robertson drove Cerebral's decision to exploit users' PHI without their consent in scores of targeted advertisement campaigns. Robertson knew that these advertisement services relied on exploiting user PHI in order to (1) re-target current Cerebral users with additional advertisements for Cerebral services, and (2) target new, potential users who were demographically similar to existing Cerebral users. Robertson directed these activities as part of an aggressive marketing strategy that aimed to barrage current users, and potential new users, with online ads—including through search engines and social media platforms such as Google, Facebook, and TikTok. At his direction, Cerebral poured significant sums of money into its targeted advertisement campaigns and made targeted advertisements a centerpiece of its strategy for achieving continued growth.

57. In directing these targeted advertisement campaigns, Robertson flouted the company's express assurances to users while sacrificing their privacy interests to grow the company and expand its subscriber base.

58. In addition to directing these activities, Robertson was personally involved in developing the company's use of tracking pixels and advertisement campaigns drawing on user PHI to target ads to users who might be more likely to engage or purchase something based on that previous online behavior. Tracking pixels can be hidden from sight and can track and send various personal data, like how a user interacts with a web page including specific items a user has purchased or information users have typed within a form while on the site.

59. Reflecting Robertson's direct control of these activities, some or all of Cerebral's

targeted advertisement service accounts were set up under Robertson's name and email address. He regularly accessed these company account pages to monitor the performance of the scores of Cerebral's simultaneous targeted advertisement campaigns that reached millions of people and to inform his discussions with subordinates about advertisement strategy.

60. For instance, Robertson was significantly involved in Cerebral's initial roll-out of targeted advertisement campaigns. According to a July 2019 Cerebral project plan for its targeted advertisement initiative, he reviewed the ads to be deployed, selected advertisement copy, helped to direct "Pixel placement" on Cerebral's website, and helped to manage the upload of approved ads to Facebook's advertisement platform.

61. The plan also reflects that Robertson had personally consulted a third-party growth agency to seek advice on best practices for targeted advertisement campaigns, including how many campaigns to launch and how best to strategize regarding effective "Audience targeting."

62. Additionally, Robertson helped formulate the company's ad strategy, developed copy for ads, decided what demographics to target, weighed in on which health conditions and aesthetic style to employ, and adjusted Cerebral's investments as between third-party platforms based on results.

63. Cerebral's use of Facebook's targeted advertisement services included marketing features that—drawing on personal data harvested from Cerebral website users and subscribers—targeted potential users by using personal identifiers of individuals who had watched Cerebral videos. The marketing features also targeted "Email List Lookalike

Audiences" based on email addresses culled from users, "Conversion Lookalike Audiences" based on personal identifiers of individuals who had completed discrete actions on Cerebral's website, and "Page Like Lookalike Audiences" based on personal identifiers of users who had "liked" Cerebral account pages.

64. Under Robertson's direction, Cerebral's use of PHI to guide its targeted advertisement campaigns extended to data such as whether a user's online activity demonstrated interests in particular mental health conditions, behavioral issues, or antidepressants. Robertson knew that this information was of a highly personal and sensitive nature and knew that users did not knowingly disclose it to the company for its own marketing purposes, or for general use by third-party marketing services.

65. Robertson regularly provided detailed input and strategic guidance regarding approval of ads, analysis of ad campaigns, and spending decisions on targeted ads.

66. Cerebral received and reviewed some online marketing service providers' written requirements that their clients (such as Cerebral) would not use or disclose user data to them without first obtaining the relevant users' authorized, informed consent for this disclosure to "third parties to perform services on your [Cerebral's] behalf…"

67. Robertson and Cerebral embarked on this sweeping advertisement strategy without clearly and conspicuously informing Cerebral's patients that their PHI would be used in this manner, and without obtaining their informed consent. In fact, to the contrary, Cerebral had assured its patients their *PHI will not be used for any other purpose, including marketing, without their consent.*

68. Moreover, Robertson persisted in this unauthorized and surreptitious exploitation of user PHI throughout his tenure at the company—for more than two-and-a-half years. During his tenure as CEO, Cerebral never notified users of the misuse of their PHI through targeted advertisement services or curtailed that misuse.

69. By permitting tracking tools on Cerebral's websites and apps, Defendants caused a massive disclosure of consumers' remarkably sensitive PHI directly or indirectly to twenty or more third parties, including LinkedIn, Snapchat, and TikTok. That information includes names; home addresses; email addresses; phone numbers; birthdates; other demographic information; IP addresses; medical and prescription histories; pharmacy and health insurance information; and other health information, including treatment plans and treatment appointment dates. Defendants disclosed or caused to be disclosed not only the identities and persistent identifiers of consumers who contacted Cerebral to seek discreet treatment from online care providers precisely because their medical treatment would be virtual (not in-person), but also detailed responses provided by consumers who completed Cerebral's intake assessment, and details of the specific treatment plans to which consumers subscribed.

70. In March 2023, over three years after it began to unlawfully share its patients' PHI with third parties as alleged above, Cerebral filed a notice with the U.S. Department of Health and Human Services ("HHS") acknowledging that its inappropriate use of tracking tools on its websites and apps constituted a breach of unsecured health information protected under HIPAA. Cerebral disclosed that its breach impacted nearly ***3.2 million consumers*** between October 2019 and March 2023.

71. Cerebral further admitted that it disclosed consumers' sensitive PHI to entities that were not able to meet all legal requirements to protect consumers' health information.

C. Defendants' Deceptive and Unlawful Data Security Practices

72. Defendants have failed to implement and maintain appropriate safeguards to prevent unauthorized access to consumers' sensitive data.

73. During Robertson's tenure as CEO, numerous Cerebral employees warned him of information security risks to consumer data in the company's possession. Despite those warnings, during and since Robertson's tenure, Cerebral has repeatedly mishandled and exposed that data in a series of data breaches.

1. Cerebral Has Mishandled and Exposed Patients' Sensitive PHI, Contrary to Its Prior Security Assurances to Them

a. Unauthorized Disclosure of Hundreds of Patient Files to Other Patients

74. Between June 23, 2021 and August 5, 2021, Cerebral released the confidential medical files of 880 patients to persons unauthorized to receive or view those files. These files contained patient names, addresses, dates of birth, diagnoses, medications, medical professionals' names, progress notes, insurance data, medical records data, and biometrics (facial photographs).

75. This information was contained in a shared electronic folder, which unauthorized persons whom Cerebral has been unable to identify accessed multiple times. Moreover, the sensitive information contained in that file was downloaded on at least one occasion.

b. Unauthorized Disclosure of Hundreds of Patient Files to Former Employees and Contractors

76. For over half a year, between at least May 11, 2021 and December 20, 2021, Cerebral allowed former employees and contractors access to the confidential electronic medical records of patients. During this period, former employees and contractors accessed 266 patient files using access credentials Cerebral failed to revoke.

77. The information accessed by these former employees and contractors included patient names, addresses, dates of birth, phone numbers, email addresses, diagnoses, treatments, prescriptions, and other health information.

78. Although Cerebral detected this breach on October 6, 2021, it allowed the breach to persist for ten more weeks, until December 20, 2021.

79. In January 2022, Cerebral ascertained that over 25% of its active or accessible login accounts for its medical records system belonged to former agents. At that time, it found that 80 agents had accessed its electronic medical records system after their departures including 13 former agents who accessed the system more than 21 days after their departures – and one former agent who accessed the system 197 days after departure.

c. Unauthorized Disclosure of Other Patient Records to Former Agents

80. On January 6, 2022, Cerebral separately found that former employees or contractors had accessed patients' medication management records more than six days after the individuals had been terminated. These former employees or contractors accessed screen tabs that displayed information for 19 patients, including patients' names, email addresses,

medications, refill dates, and/or other sensitive PHI.

d. Unauthorized Postcards Revealing Thousands of Patients in Treatment

81. On July 25, 2022, Cerebral caused promotional postcards to be sent to approximately 6,100 patients, inviting them to participate in a research study. The postcards included the names and addresses of patients in treatment, and language that reasonably indicated diagnosis, treatment, and a relationship with Cerebral. Since Cerebral did not send the postcards in an envelope, the postcards overtly revealed patients' private, HIPAA-protected status as patients obtaining treatment, and exposed this information to anyone who saw the postcards.

e. Unauthorized Logins to Other Patients' Files

82. In at least September 2022, Cerebral utilized a single sign-on ("SSO") method for access to its patient portal. In numerous instances, this method exposed confidential medical files and patient information to other patients when those users signed onto the portal nearly simultaneously.

83. The information revealed in these data breaches included patient names, email addresses, addresses, phone numbers, diagnoses, medications, medical professionals' names, upcoming appointments, chat history, medical record numbers, the last four digits of the credit card on file, and the card expiration date. These breaches occurred after Cerebral had notice of the FTC investigation that led to this case.

84. Cerebral was apparently unaware of these breaches until a patient called to report that his medical records had been revealed to a stranger who located his phone number in the file

Cerebral maintained on him and then called him.

85. In addition to the foregoing data breaches, Cerebral has exposed patients' private, HIPAA-protected health information in dozens of other instances.

86. Defendants' practices, taken individually or together, have failed to provide reasonable security to prevent unauthorized access to clients' sensitive PHI. Among other things, Defendants have:

A. failed to timely develop, implement, or maintain adequate written information security standards, policies, or procedures with respect to the handling, collection, use, and disclosure of patients' health information, including ensuring that Cerebral's practices complied with its privacy and data security representations to patients, and timely adopting and enforcing formal personnel offboarding policies;

B. failed to monitor and timely deactivate the accounts of terminated and other former agents—compounding this issue, Cerebral has acknowledged gaps in its Human Resources employment records;

C. failed to properly supervise agents, contractors, and employees with respect to their collection, use, and disclosure of consumers' sensitive PHI;

D. failed to require distinct, unique passwords, instead permitting staffers or contractors to use a single access key to obtain access to patients' electronic medical records while using Dropbox to share such records;

E. failed to exercise internal information controls necessary to prevent public disclosure of patients' treatment by Cerebral's care providers;

F. failed to restrict access to systems based on job functions, for example, allowing care providers access to sensitive personal information of many patients whom they did not treat, they were not responsible for treating, or whose information they did not need to do their jobs;

G. failed to restrict access to systems based on consumers' login credentials, permitting some patients to log into accounts using a defective sign-on process that exposed their confidential medical records to unauthorized recipients;

H. failed to implement policies and procedures to ensure the timely remediation of critical security vulnerabilities, allowing multiple breaches to persist for months and/or years;

I. failed to reasonably respond to security incidents, for example by failing to: (1) timely disclose security incidents to relevant parties; and/or (2) take prompt action upon notification of a security incident; and

J. failed to provide adequate guidance or training for staffers or contractors regarding information security and properly safeguarding personal information.

2. Robertson's Supervision of, and Direct Participation in, Cerebral's Unlawful Data Security Practices

87. During his time as Cerebral's CEO, Robertson was regularly informed about and closely involved in directing Cerebral's management of chronic data security problems.

88. He often participated in sensitive discussions about Cerebral's repeated data security problems and how to respond to them. Robertson also held formal responsibilities as one of the designated members of Cerebral's "Data Breach Response Team." Cerebral's Data Breach

Policy required that Robertson be immediately notified whenever Cerebral initiated an investigation into a data breach.

89. Through formal internal investigations and findings developed by the company, Robertson was briefed on major data security issues and involved in managing the company's formulation of its response—including through communications with Cerebral's Board, decisions as to changes in company practices, and outreach to affected users and regulators.

90. Despite Robertson's knowledge of Cerebral's chronic data security problems, he failed to ensure that the company correct those problems, mitigate data security risks, and respond appropriately to known breaches, or to live up to its assurances to users that their data was safe and secure.

91. To the contrary, Robertson shaped and approved Cerebral's annual budgets, which invested disproportionately in growth and marketing, but deprioritized compliance and data security functions. For example, in April 2022, Robertson approved a budget allocating $211 million to Cerebral's Growth Department, which managed the company's marketing and advertising strategy. By contrast, the budget provided relatively paltry funding for Cerebral's Safety & Quality (approximately $1.6 million) and Security & IT ($5.1 million) functions. Robertson approved this lopsided budget despite (a) knowing that chronic, rudimentary HIPAA compliance and data security breach issues had dogged Cerebral, and (b) that Safety & Quality and Security & IT issues should have been paramount for a telehealth company.

92. Robertson also served as the designated reviewer and approver of Cerebral's policies on data security and data breaches. He personally approved those policies.

93. Robertson's failure to prioritize basic data security safeguards, despite Cerebral's assurances to its users, included failing to ensure adequate data security compliance staffing and adequate training for company employees. As a result of his failures, Cerebral employees regularly mishandled or compromised sensitive user data under Robertson's leadership.

94. Robertson failed to adequately prioritize and address Cerebral's deficient data security practices even though his top reports monitoring the company's data security practices pinpointed critical, systemic issues. Issues identified by Robertson's reports included: data security risks related to Cerebral's sign-on mechanism; lack of adequate folder access restrictions preventing improper access to PHI; the company's use of applications for storing and transmitting PHI that were inadequate for safeguarding sensitive medical data; and partnerships with third parties with data security practices that were known to be inadequate for properly safeguarding user data under HIPAA.

95. As detailed above, these known data security issues contributed to data breaches to which Cerebral users were exposed.

96. In some instances, Robertson overrode significant data security concerns raised by his top data security reports. For example, in November 2021—after the company had experienced multiple breaches—Cerebral's Chief Information Security Office ("CISO") advised Robertson that Cerebral should not enter into a partnership with a third party with problematic data security practices. The CISO had determined that "Cerebral as a business should not have a risk appetite for this partnership…. [given the third party's] clearly poor security hygiene on their website." The CISO presented her conclusion to Robertson that the "website is not

secure/confidential information is open to the public" and that a partnership would expose users to a risk of breach. Nevertheless, Robertson determined that this risk was acceptable for Cerebral to assume.

97. Under Robertson's leadership, Cerebral made strong data security assurances to prospective users that were belied by its pervasive data security deficiencies and chronic, preventable breaches.

IV. Defendants' Deceptive and Illegal Negative Option Cancellation Practices

98. At least during Robertson's tenure as Cerebral's Chief Executive Officer, Defendants failed to clearly disclose all material terms of the transactions with consumers using a negative option feature, such as material terms about data privacy, data security, and cancellation, before obtaining consumers' billing information.

99. Defendants therefore failed to obtain consumers' express informed consent before charging the consumers' credit card, debit card, bank account, or other financial account for products or services through such transaction.

100. Defendants also failed to provide simple mechanisms for a consumer to stop recurring charges from being placed on the consumer's credit card, debit card, bank account, or other financial account.

101. In fact, Cerebral charged its clients on a recurring basis for subscriptions that automatically renewed monthly unless clients cancelled before the end of their billing cycles. Cerebral also collected several million dollars even after those clients had asked Cerebral to

cancel their subscriptions. A significant portion of that sum has never been refunded to consumers.

A. Defendants Failed to Disclose All Material Terms Before Obtaining Patients' Billing Information

102. Between late 2019 and at least May 2022, Defendants failed to clearly disclose all material terms of the transaction, such as important terms related to data privacy, data security, and cancellation before Cerebral obtained patients' billing information and before it charged them.

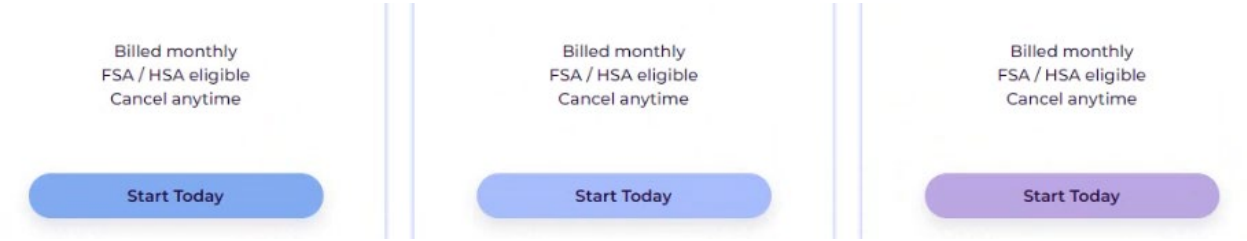
103. For instance, Defendants failed to disclose how the company's patients' PHI and other sensitive information would be used. In their repeated assurances to their patients, Defendants touted Cerebral's restrictions on the use and disclosure of consumers' sensitive data, as well as its safeguards against unauthorized disclosure of such data. In particular, Defendants assured patients that their PHI and other sensitive information would "*not be used for any other purpose, including marketing, without [their] consent.*" (emphasis added). These sorts of assurances appeared in Cerebral's promotional claims, online enrollment path, and official policies posted online. Defendants' numerous misrepresentations and omissions regarding Cerebral's privacy and data security practices encouraged consumers to disclose their sensitive PHI and subscribe to Cerebral's services. Consumers have reasonably relied on these representations or omissions. In fact, patients often seek medical care such as mental health care and substance abuse treatment online, rather than in-person, precisely because they prioritize, if not require, privacy and confidentiality.

104. But Defendants failed to clearly disclose that, in fact, they deliberately shared, or

allowed the sharing of, consumer information with numerous third parties whose services they utilized to promote Cerebral's services. That information includes, among other things, patient names; home addresses; email addresses; medical and prescription histories; detailed responses to Cerebral's intake assessment, and details of patients' specific treatment plans.

105. Likewise, Defendants failed to disclose material terms about cancellation. As part of its enrollment process, Cerebral represented that clients may "Cancel anytime." For example, in many instances, the landing pages of Cerebral's websites or apps included the text, "Cancel anytime."

106. This "Cancel anytime" claim appeared repeatedly, including three times on a single page, on Cerebral's website or app screens describing its treatment plans, immediately above the button consumers may click to start the enrollment process:



107. In many instances, this "Cancel anytime" claim appeared again on the screen consumers may use to confirm their treatment plan selection.

108. Cerebral's online enrollment path on its websites and its mobile apps required consumers to provide contact and payment information to subscribe to its treatment plans on its checkout page. It collected such information above a button with a label such as "Submit," referenced earlier. Below that button, fine print text mentioned a cancellation policy, but in many instances, omitted material terms about cancellation.

109. Until May 2022, Cerebral's cancellation terms appeared only in separate areas of its websites and apps – such as a page on its websites in the middle of a list of answers to Frequently Asked Questions ("FAQ"), on a Help webpage, or in its lengthy terms and conditions.

110. In May 2022, more than two and half years into its business operations, Cerebral introduced an iteration of its final checkout page that displayed more information concerning its cancellation terms in the enrollment path. The text stated, in pertinent part: "Cancel by emailing cancel@cerebral.com by 9 a.m. PT before your next billing date to avoid future charges."

B. To Reduce Patients' Cancellations, Cerebral—at Robertson's Direction—Deliberately Failed to Provide Simple Mechanisms for Patients to Cancel and Stop Recurring Charges

111. Cerebral has represented that its patients can contact it by email, text, or phone and that its representatives are available from 6am-6pm PT Monday through Friday and from 7am-4pm PT Saturdays and Sundays. It has also represented that all of its customers will "receive a response within one business day." However, these representations did not apply to its cancellation process. Instead, at nearly all points between October 2019 and May 2022, Cerebral required its clients to navigate a burdensome, complex, lengthy, multi-step, and often multi-day process to cancel their subscriptions and to stop recurring charges.

112. From October 2019 to April 2020, Cerebral claimed clients "may cancel [their] subscription[s] at any time by contacting Support (support@getcerebral.com)." However, emailing a cancellation demand did not actually cancel a subscription or stop recurring charges. Instead, Cerebral systematically subjected many clients to a lengthy and burdensome "save"

process in which its staff contacted them with questions and attempted to dissuade them from cancelling. Until this process ended, and Cerebral's staff "confirmed" consumers' cancellation demands, clients' subscriptions remained active, and the clients remained subject to additional charges.

113. For approximately two weeks in mid-to-late April 2020, Cerebral provided a cancellation mechanism that enabled clients to cancel subscriptions by logging into their online Cerebral profile and clicking a cancellation button located in their profile by 5pm PT the business day before their next scheduled billing date. Robertson remarked that he was concerned that that cancellation design made it "really easy to keep hitting 'Continue with cancellation." Defendants indeed found that this mechanism increased their customers' cancellation rate. Cerebral terminated the mechanism at Robertson direction.

114. In early May 2020, Cerebral reinstated the requirement that clients submit their cancellation demands by email to support@getcerebral.com. Further, after July 2020, Cerebral made the cancellation process more burdensome by declining to honor cancellation demands made through channels other than the email account specified for cancellation, directing clients to resubmit their demands via email. Cerebral further retained the requirement that clients email cancellation demands by 5pm PT the business day before their next scheduled billing date. It also resumed its practice of seeking to question, dissuade, and "save" clients who made cancellation demands. As before, until Cerebral's "confirmation" of clients' demands, clients remained subject to further charges.

115. Cerebral introduced numerous other changes to its cancellation terms and process

in October 2020 and thereafter. On October 16, 2020, for example, Cerebral revised its policy to require clients to email support@getcerebral.com by 9am PT two business days before their next scheduled billing date to demand the cancellation of their subscriptions. Four days later, Cerebral revised its policy to require clients to email cancellation demands one business day before their next scheduled billing date to cancel. On November 1, 2020, Cerebral again changed its cancellation email address, requiring clients to email cancel@getcerebral.com by 9am PT one business day before their next scheduled billing date to cancel. On December 17, 2020, Cerebral yet again changed its cancellation email address, once again advising clients to email its general support email inbox, support@getcerebral.com, now by 5pm PT the business day before their next scheduled billing date to cancel. On February 2, 2021, Cerebral again revised its cancellation terms to require clients to email cancel@getcerebral.com by 9am PT the business day before their next scheduled billing date to cancel. Cerebral imposed these terms on all of its clients, who did not necessarily know of the changes.

116. At the end of May 2022, Cerebral finally revised its cancellation process to permit clients again to cancel their subscriptions by clicking a cancellation button.

117. In May 2022, after Robertson was no longer CEO, an internal Cerebral message, copied to seven people, including its President and Chief Operating Officer, stated with regard to the expected business impact of re-introducing an online cancellation button for users: "Business impact: . . . 5-20% Expected increase in cancellation requests and voluntary churn . . . somewhat unavoidable given we want to make this change for compliance purposes."

118. In addition to these cancellation requirements, Cerebral imposed other

challenging and burdensome requirements on patients trying to cancel. In October 2020, Cerebral modified its cancellation process to introduce a detailed cancellation assessment that it directed clients seeking to cancel to complete. This assessment replaced the questions its staff asked clients between at least January and October 2020. In this new process, when clients demanded cancellation, Cerebral emailed them a link to an assessment. The assessment changed over time but was dynamic so clients could be prompted to answer additional questions based on their prior answers.

119. Some iterations of the assessment required clients to respond to statements by clicking a "Proceed with Cancellation" button to remain on the cancellation path. Other iterations of the form asked clients to confirm their email address and the state in which they were located; indicate whether they met with one of Cerebral's providers before demanding cancellation; select a reason for their cancellation from a list; answer a follow-up question about their experience based on the cancellation reason selected; indicate whether they would continue to receive mental health treatment after discontinuing treatment through Cerebral, and if so, for what conditions; indicate whether they were interested in discussing non-stimulant medication with their prescriber; answer whether they would accept a discount for continued treatment instead of cancelling and potentially answer a follow-up question; indicate whether they would like to speak directly with a coordinator to discuss a personalized solution or discount in lieu of cancelling; and/or asked for additional feedback regarding their experience with Cerebral.

120. The form also asked clients to identify the plan they intended to cancel. However, the list of plans did not consistently match the list of plans presented to clients when they

subscribed.

121. Cerebral continued to use some version of its detailed cancellation assessment through at least April 2022. In some instances, Cerebral contacted clients to further dissuade or "save" clients who made cancellation demands even after they submitted a cancellation demand and completed the cancellation assessment.

122. After receiving a completed cancellation assessment, Cerebral advised clients, in pertinent part, "Please allow up to 1-2 business days for processing[.]" This admonition did not appear in Cerebral's online enrollment path, FAQ, or terms. Moreover, Defendants failed to otherwise clearly or accurately disclose this information to clients before Cerebral obtained its patients' billing information and before it charged them. During this "processing" period, clients remained subject to further charges, and Cerebral took additional monthly subscription payments from consumers who had completed cancellation assessments. Moreover, Cerebral did not always process a completed cancellation assessment within 1-2 business days, and charged some clients beyond the timeframes in which it represented it would process completed assessments.

123. Even compliance with Cerebral's changing cancellation requirements did not ensure clients could timely cancel recurring charges. In over 56,000 instances, Cerebral charged clients after clients demanded the cancellation of their subscriptions and submitted a completed cancellation assessment.

124. Between October 2019 and May 2022, Cerebral collected over $8 million from consumers after receiving their cancellation demands. A substantial portion of this amount was never refunded.

C. Robertson Was Extensively Involved in Cerebral's Deceptive and Unlawful Cancellation Process

125. Given his prioritization of growing Cerebral's subscriber base, Robertson focused significantly on minimizing the loss of paying subscribers to Cerebral's telehealth services.

126. Accordingly, Robertson was especially attuned to supervising Cerebral's design of its cancellation process. Robertson understood—and sought to ensure that his subordinates understood—that creating obstacles to user cancellation was a key tool for Cerebral's maintenance of its subscriber base.

127. To this end, Robertson closely managed Cerebral's cancellation flow, and his approval was required for overarching changes to the cancellation design. Teams discussing experimenting with changes to Cerebral's cancellation flow openly highlighted the need for Robertson's approval before any changes could be made.

128. Robertson participated directly on teams that analyzed and designed Cerebral's cancellation process. He tested Cerebral's cancellation design, gave guidance about its design, and issued directions to his subordinates about Cerebral's cancellation approach. For example, in April 2020, Robertson highlighted to a Cerebral user-experience designer his concern that Cerebral's current cancellation design made it "really easy to keep hitting 'Continue with cancellation,'" and advocated redesigning the flow in order to make it harder for users to cancel.

129. Robertson also warned his subordinates that "the churn has gotten much worse since moving over to letting client cancel on their own, rather than emailing for cancellation." Because making cancellation simpler had increased patients' cancellation, or "churn," Robertson explained that it might be necessary to "move back to the old cancellation process if the data

doesn't change dramatically here."

130. In April 2020, Robertson also explained to his employees that it was imperative they determine "what cancellation flow is best," meaning "which cancellation flow is best for minimizing churn." In other words, he ordered that the cancellation process be measured by determining what process led to fewer cancellations.

131. In May 2020 Robertson directed his subordinates to require users to use email to cancel their subscriptions because "the data directionally highlighted that the email cancellation flow has lower churn"

132. Ultimately, Robertson pursued his agenda of ensuring a complex cancellation process that would make it more burdensome and difficult to cancel by ordering that Cerebral remove the cancellation button.

133. Following removal of the cancellation button, one Cerebral employee informed another that "[t]here is no way… Kyle [Robertson] would sign off … on rolling out a cancellation button [following its removal] *without data that it wasn't going to drive up # of cancellations*…" (emphasis added).

134. Under Robertson's leadership, Defendants removed the cancellation button despite knowing that it streamlined the cancellation process in a way that was user-friendly and avoided instances of erroneous billing. This deliberate removal of the cancellation button was in stark contrast to consumers' ability to enroll in Cerebral's services (and become subject to automatic payments under its negative option) with a few simple clicks of buttons.

135. Cerebral's decision under Robertson's command to remove the cancellation

button was consistent with the company's general approach of making cancellation unnecessarily complex, frustrating, and uncertain—for instance, by requiring a complex, multi-step process for cancellation rather than simply honoring emails from users stating unequivocally that they sought to cancel their subscriptions.

136. Cerebral's deliberate creation of challenges to cancellation included insisting that users could cancel by reaching out to only a specific support email address that required time-consuming interactions with a live agent. Under Robertson's direction, Cerebral insisted on maintaining this burdensome approach—opposing automation of the cancellation process after conducting detailed analysis of that possibility—in order to reduce cancellations by making them more challenging for users and equipping Cerebral with the opportunity to "save" users from cancelling.

137. Robertson controlled Cerebral's cancellation strategy from top to bottom. He was briefed on all relevant aspects of Cerebral's cancellation flow through Slack discussions, detailed analyses presented by his reports, and through participation in tech prioritization meetings discussing cancellation and churn issues.

138. He repeatedly directed employees to introduce obstacles and challenges into Cerebral's cancellation process. This served the company's goals of minimizing churn and reducing the number of refunds Cerebral was required to pay.

139. Robertson exercised his control over Cerebral's cancellation process to ensure that it would remain complicated, challenging, and frustrating for users to try to cancel—flouting Cerebral's assurance to users that they would be able to "cancel anytime," and knowingly

flouting Cerebral's ROSCA obligations in the process.

D. Defendants Knew of Consumer Complaints Arising from Their Deliberate Decision to Make Cancellation Complex and Challenging

140. Defendants knew that their intentional refusal to provide a simple mechanism for cancellation caused a large number of consumer complaints.

141. Robertson was repeatedly briefed on widespread consumer complaints in app stores, social media sites, and online review sites regarding frustration with their unsuccessful attempts to cancel—and the hefty monthly fees they were often charged after those attempts.

142. When Cerebral employees tested out the cancellation flow for themselves, they ran into the same hurdles and frustrations encountered by users. For instance, a Cerebral employee who tried to follow the cancellation directions in March 2022 reported to colleagues that "the process is a long (and tedious) user experience" and "In short, its (sic) a burden." The employee highlighted the lack of a cancellation button, the arbitrary requirement to email a support address, and the need to then wait for a response and subsequent steps—with no clarity as to timing or the nature of the remaining process to be completed.

143. Similarly, a February 28, 2022 message on Cerebral's internal Slack messaging platform, copied to fifteen people, including members of its executive team, stated in pertinent part: "[T]here are multiple points of failure with the current cancelation [*sic*] flow, and the difficulty of canceling consistently frustrates clients month over month[.]"

144. Robertson was informed by colleagues of routine consumer frustrations with thwarted attempts to cancel as well as clients being charged after cancellation.

145. Cerebral carefully tracked statistical trends among consumer complaints, and so knew of widespread consumer frustration with its deliberately challenging cancellation process.

146. Cerebral also frequently received impassioned messages directly from users outlining their frustrations in trying—and apparently failing—to cancel their subscriptions.

A. For instance, one user who emailed Cerebral more than half a dozen times trying to cancel her subscription finally wrote to the company: "Y'know, as a company that deals with anxiety you should probably understand how anxiety inducing it is to have no control over the cancellation of a subscription when you're stuck in the middle of a process and can't get in or out of it and you have your credit card already in the system." In a follow-up email, she added: "If you cared about people's mental health you wouldn't send them in circles and scam them."

B. Another user emailed the company that she had been trying to cancel for two weeks and had yet to receive any response: "I have been trying to cancel for like 2 weeks and haven't heard anything. I do not want to be charged again seeing as I was charged for literally nothing."

C. Another user complained that they had emailed their cancellation request early in the month yet were still charged $300 at month's end: "I did everything I was supposed to. Quit taking money from my account!!!!!!!"

D. A similarly frustrated user wrote to the company that this was their "3rd time through email" attempting to cancel and demanded the company cancel her subscription.

E. Still another user lambasted the company for misleading her in making its upfront guarantee that she would be able to "cancel anytime," when clearly this was not the case: "Why would [my cancellation request] be reviewed when you specifically said that I can cancel at any time. You didn't say 'cancel any time after your subscription will be reviewed'. I want you to refund me immediately or I will take further action. Your advertisements is false … [I] was told 'you can cancel any time' … you provide false advertisement … you specified CANCEL ANYTIME not CANCEL AFTER WE REVIEW YOUR SUBSCRIPTION FOR CANCELLATION. And the crazy part is that this app this service supposed to help people. I want my money to be REFUNDED right away. Stop scamming people."

147. Cerebral's negative option cancellation practices have generated especially pointed complaints from clients struggling with Attention-Deficit/Hyperactivity Disorder ("ADHD"). For example, one consumer complaint stated: "I find it appalling that a mental health care app/company that serves those with ADHD would make you jump through hoops to cancel like this - it's just the thing people with ADHD typically find challenging to manage and seems predatory." Similarly, another consumer stated: "Cancel[l]ation is extremely difficult and patients are unable to see if their cancellation has processed. The cancel[l]ation process seems to be tailor made to stop a person with ADHD from being able to complete the task."

148. When consumers believe that they have been subject to unfair business practices, or when merchants fail to provide refunds that consumers are entitled to or make such refunds

difficult to obtain, consumers may choose to dispute specific charges on their credit cards by seeking what is commonly known as a "chargeback." Card networks, such as Visa, set thresholds for excessive chargebacks, and merchants that exceed the card network thresholds are subject to additional monitoring requirements.

149. During 2020 and through early 2021, Cerebral was placed in the Visa Dispute Monitoring Program, a monitoring program established by Visa to identify merchants with a high level of customer disputes. Through May 2022, Cerebral's rate of chargebacks was consistently above 0.5% and often exceeded 1%, a rate that banks and financial organizations generally treat as requiring heightened scrutiny for possible fraud.

V. Defendants' Ability and Incentive to Continue Their Unlawful Conduct

150. Based on the facts and violations of law alleged in this Complaint, including the allegations set forth above, the United States has reason to believe that Defendants are violating or are about to violate the laws identified in this Complaint. Defendants engaged in their unlawful acts and practices repeatedly over a period of years and at least since the inception of their marketing activities. Further, they retain the means, ability, and incentive to continue their pattern of unlawful conduct in the telehealth space. Cerebral remains operational and continues to possess PHI and use a negative option feature.

151. In 2023, Robertson founded a Florida corporation that operates as a telehealth company with a corporate address in this District. He has stated that company will, purportedly like Cerebral before it, "improv[e] high quality healthcare at scale." The company has publicly offered mental health care (including treatment for anxiety and depression) and other health care

services (such as weight loss treatment, and treatment for erectile dysfunction and hair loss) to consumers on a subscription basis. This company has made representations relating to privacy, confidentiality, and data security while collecting consumers' sensitive personal information for marketing, sales, or other promotional purposes. Like Cerebral, it also promotes and sells its services through a negative option feature. And, like Cerebral, it uses a rapid, online sign-up process that asks users to enter their payment information for subscription billing without first clearly disclosing and obtaining consent to all material terms of the service.

152. Robertson has hired several ex-Cerebral employees to fill critical, early roles at his new company—including an engineer, an operations manager, and a clinical care manager. In just the short time since that company has been operating, people claiming to be the company's customers have posted detailed online complaints alleging misconduct similar to Cerebral's misconduct described above.

153. In particular, customers claim that the company has made it very challenging to cancel their subscriptions. For instance, one person recently complained that the company required "15 prompts to cancel and to cancel is only thru an app. They still will not refund you and just state "that [*sic*] your membership is now scheduled to be canceled." Another person claiming to be the company's customer recently complained that he "asked several times to cancel and they finally sent me a link to cancel but it does not work."

154. Customers have also complained about significant undisclosed charges, recurring charges they did not knowingly consent to, and misleading representations made during the sign-up process regarding the services that would be included in the plans they signed up for.

155. A March 2024 job listing for a marketing role at Robertson's new company also indicates that the company is already using—or plans to use—the same third-party websites and social media platforms that Cerebral used to facilitate its targeted advertisements under Robertson's direction.

156. That Robertson's new company has apparently engaged in similar conduct as Cerebral did under his direction—even in the face of a government investigation into his role in those very practices as Cerebral's CEO—squares with Robertson's refusal to accept any responsibility for it when Cerebral ousted him. Internal Cerebral documents show that, in the months leading up to Robertson's termination, top company executives discussed their concerns that his flouting of safety and compliance issues was imperiling the company's future and that he might need to be pushed out in order to save the company. Despite these views within the company, Robertson's public declarations after his firing refused to accept any responsibility and instead argued that he was being unfairly scapegoated and subjected to an illegal termination.

157. Given Robertson's refusal to accept responsibility or to acknowledge compliance issues under his leadership at Cerebral, there is reason to believe that he will continue to break the law until he is forced to stop. Indeed, consumer reviews regarding his new telehealth company suggest that he is doing so as of this filing.

158. Absent injunctive relief, Defendants are likely to continue their unlawful conduct.

COUNT I

FTC Act Section 5—Deceptive Privacy Practices

159. Paragraphs 1 through 158 are incorporated as if set forth herein.

160. In numerous instances, in connection with the promotion or sale of services offering online health care or treatment, such as mental health treatment or substance use disorder treatment services, Defendants have represented, directly or indirectly, expressly or by implication, that:

A. Cerebral's service is private or confidential;

B. Cerebral keeps consumers' personal information private or confidential;

C. Cerebral keeps consumers' health care or treatment private or confidential;

D. Cerebral would not use consumers' personal information, including PHI, for marketing purposes or other purposes without consumers' consent;

E. Cerebral would not disclose consumers' personal information, including PHI, without consumers' consent; and

F. Cerebral would not disclose consumers' personal information, including PHI, to third parties for marketing purposes or other purposes without consumers' consent.

161. Each of the above-listed representations in paragraphs 160 (A)-(F) constituted terms that were material to consumers.

163. In truth and fact:

A. Cerebral's service was not, or is not, private or confidential;

B. Cerebral has not kept consumers' personal information private or confidential;

C. Cerebral has not kept consumers' health care or treatment private or confidential;

D. Cerebral has used consumers' personal information, including PHI, for marketing purposes or other purposes without consumers' consent;

E. Cerebral has disclosed consumers' personal information, including PHI, without consumers' consent; and

F. Cerebral has disclosed consumers' personal information, including PHI, to third parties for marketing purposes or other purposes without consumers' consent.

164. This conduct, as alleged in paragraphs 163 (A)-(F), shows that Defendants' representations were deceptive.

165. Therefore, Defendants' acts or practices set forth above constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

COUNT II

FTC Act Section 5—Deceptive Data Security Practices

166. Paragraphs 1 through 165 are incorporated as if set forth herein.

167. In numerous instances, in connection with the promotion or sale of services offering online health care or treatment, such as mental health treatment or substance use disorder treatment services, Defendants have represented, directly or indirectly, expressly or by implication, that:

A. Cerebral keeps consumers' personal information, including personal health information, secure;

B. Cerebral fully secures or safeguards consumers' personal information, including PHI, from unauthorized or unconsented access, use, or disclosure;

C. Cerebral implemented reasonable measures to protect consumers' personal information, including PHI, against unauthorized or unconsented access, use, or disclosure; and

D. Cerebral collects personal information from consumers, including PHI, in a secure manner.

168. In truth and fact:

A. Cerebral has not kept consumers' personal information, including PHI, secure;

B. Cerebral has not fully secured or safeguarded consumers' personal information, including PHI, from unauthorized or unconsented access, use, or disclosure;

C. Cerebral did not implement reasonable measures to protect consumers' personal information, including PHI, against unauthorized or unconsented access, use, or disclosure;

D. Cerebral collects personal information from consumers without ensuring that it is protected in a secure manner; and

E. Defendants have failed to disclose, or disclose adequately to consumers, that Cerebral has not kept consumers' personal information secure, fully protected that information against unauthorized or unconsented access, use, or disclosure, or did not implement reasonable measures to protect that information against unauthorized or unconsented access, use, or disclosure. This additional information would have been material to consumers in deciding whether to purchase or use Cerebral's services.

169. Therefore, Defendants' acts or practices as set forth above constitute deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a).

COUNT III

FTC Act Section 5—Unfair Privacy and Data Security Practices

170. Paragraphs 1 through 169 are incorporated as if set forth herein.

171. In numerous instances, in connection with the promotion or sale of services offering online health care or treatment, such as mental health treatment or substance use disorder treatment services, Defendants have:

A. Failed to employ reasonable measures to protect consumers' personal information, including PHI, in connection with the collection, use, or disclosure of that information, resulting in the improper and unauthorized disclosure of that information to numerous third parties; and

B. Used consumers' PHI for marketing purposes or other purposes, or disclosed consumers' PHI to third parties to use for marketing purposes or other purposes, without obtaining consumers' affirmative express consent to use, or to disclose to third parties to use, their PHI for marketing purposes or other purposes.

172. Defendants' acts or practices as set forth above 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.

173. Therefore, Defendants' acts or practices as set forth above constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

COUNT IV

FTC Act Section 5 Violations—Deceptive Cancellation Practices

174. Paragraphs 1 through 173 are incorporated as if set forth herein.

175. In numerous instances, in connection with the promotion or sale of services offering online health care or treatment, such as mental health treatment or substance use disorder treatment services, Defendants have represented, directly or indirectly, expressly or by implication, that consumers can "Cancel anytime."

176. In truth and fact, Defendants did not allow consumers to cancel at any time. Instead, for over two years, the vast majority of consumers could only demand cancellation. Consumers then had to undergo Cerebral's "save" process: Cerebral required consumers to send emails, answer verbal questions or fill out detailed assessment forms, and/or wait days for their cancellation demands to be satisfied, during which time consumers were subjected to further recurring charges, and, in many instances, paid money to Cerebral before Cerebral actually cancelled their subscriptions.

177. Therefore, the making of these representations constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT V

Violations of the Opioid Act

178. Paragraphs 1 through 177 are incorporated as if set forth herein.

179. Defendants' unfair or deceptive acts or practices set forth above regarding data security and data privacy constitute unfair or deceptive acts or practices with respect to a substance use disorder treatment service in violation of Section 8023(a) of the Opioid Act, 15 U.S.C. § 45d(a).

180. Defendants violated the Opioid Act with the requisite knowledge – actual knowledge or knowledge fairly implied on the basis of objective circumstances – to be liable for civil penalties under Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

COUNT VI

Violations of the Restore Online Shoppers' Confidence Act

181. Paragraphs 1 through 180 are incorporated as if set forth herein.

182. As described in above, Defendants have promoted and sold services offering online health care treatment or "telehealth," including mental health treatment, medication management, or substance use disorder treatment services, through a negative option feature as defined by the TSR. 16 C.F.R. § 310.2(u).

183. In numerous instances, in connection with charging or attempting to charge consumers for services offering online health care treatment sold in transactions effected on the Internet through a negative option feature, Defendants have failed to:

A. Clearly and conspicuously disclose all material terms of the transaction before obtaining the consumer's billing information, including terms related to data security, data privacy, and cancellation as described above; and

B. Obtain a consumer's express informed consent before charging the consumer's credit card, debit card, bank account, or other financial account for products or services through such transaction; or

C. Provide simple mechanisms for a consumer to stop recurring charges from being placed on the consumer's credit card, debit card, bank account, or other financial account.

184. Defendants' acts or practices described above violate Section 4 of ROSCA, 15 U.S.C. § 8403, and are thus treated as violations of a rule promulgated under Section 18 of the

FTC Act, 15 U.S.C. § 57a, 15 U.S.C. § 8404(a), and therefore constitute an unfair or deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

185. Defendants violated ROSCA with the requisite knowledge – actual knowledge or knowledge fairly implied on the basis of objective circumstances – to be liable for civil penalties under Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

CONSUMER INJURY

186. Consumers have suffered and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act, the Opioid Act, and ROSCA. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers and harm the public interest.

PRAYER FOR RELIEF

187. Wherefore, Plaintiff requests that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act, the Opioid Act, and ROSCA by Defendants;

B. Award monetary civil penalties from Defendants for every violation of the Opioid Act and ROSCA;

C. Award monetary and other relief within the Court's power to grant; and

D. Award any additional relief as the Court determines to be just and proper.

DEMAND FOR JURY TRIAL

The United States hereby demands a jury trial on all claims alleged herein.

Dated: April 12, 2024

Respectfully submitted,

FOR THE FEDERAL TRADE COMMISSION:

Joshua S. Millard
Christopher J. Erickson
Attorneys
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mailstop CC-6316
Washington, D.C. 20580
(202) 326-2454 (Millard)
(202) 326-3671 (Erickson)
(202) 326-3197 (Facsimile)
jmillard@ftc.gov
cerickson@ftc.gov

FOR THE UNITED STATES OF AMERICA:

Brian M. Boynton
Principal Deputy Assistant Attorney General
Civil Division

Arun G. Rao
Deputy Assistant Attorney General

Amanda N. Liskamm
Director

Rachael L. Doud
Assistant Director

/s/ Shana C. Priore
Shana C. Priore
Francisco L. Unger
Joshua A. Fowkes
Trial Attorneys
Consumer Protection Branch
U.S. Department of Justice
450 5th Street, N.W. Suite 6400-South
Washington, D.C. 20044
202-598-8182 (Priore)
202-742-7111 (Unger)
202-532-4218 (Fowkes)
202-514-8742 (Facsimile)
Shana.C.Priore2@usdoj.gov
Francisco.L.Unger@usdoj.gov
Joshua.A.Fowkes@usdoj.gov

Markenzy Lapointe
United States Attorney
Southern District of Florida

Rosaline Chan
Assistant United States Attorney
Fla. Bar No. 1008816
United States Attorney's Office

99 N.E. 4th Street
Miami, Fl. 33132
Phone: (305) 961-9335
Rosaline.Chan@usdoj.gov