UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Case No. 24-cv-21376-KING/REID

UNITED STATES OF AMERICA,
Plaintiff,
v.
CEREBRAL, INC., a corporation, et al.,
Defendants.

JOINT STIPULATION FOR ORDER FOR PERMANENT INJUNCTION, MONETARY JUDGMENT, CIVIL PENALTY JUDGMENT, AND OTHER RELIEF AGAINST DEFENDANT CEREBRAL, INC

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("Commission" or "FTC"), filed its Complaint for Permanent Injunction, Monetary Relief, Civil Penalties, and Other Relief ("Complaint") for a permanent injunction, monetary relief, civil penalties, and other relief in this matter, pursuant to Sections 13(b), 19, and 16(a)(1) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 53(b), 57b, and 56(a)(1); 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. Defendant Cerebral, Inc. has waived service of the summons and the

Complaint. Plaintiff and Defendant Cerebral, Inc. stipulate to the entry of this Stipulated Order for Permanent Injunction, Monetary Judgment, Civil Penalty Judgment, and Other Relief ("Order") to resolve all matters in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.

2. The Complaint charges that in connection with the promotion or sale of services offering online health care treatment, such as mental health treatment or substance use disorder treatment services, Defendant Cerebral, Inc. participated in deceptive and unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, and Section 8023(a) of the Opioid Act, 15 U.S.C. § 45d(a). The Complaint further charges that in connection with charging or attempting to charge consumers for its services, Defendant Cerebral, Inc. violated Section 5 of ROSCA, 15 U.S.C. § 8404.

3. Defendant neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Order. Only for purposes of this action, Defendant admits the facts necessary to establish jurisdiction.

4. Defendant waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorney fees.

5. Defendant waives all rights to appeal or otherwise challenge or contest the validity of this Order.

DEFINITIONS

For the purpose of this Order, the following definitions apply:

A. **"Acquisition"** means the purchase of one company by another. An Acquisition may be structured as an acquisition of stock, assets (including the acquisition of applications or websites, contracts, patents, intellectual property, or data), talent (*e.g.*, employees or agents), or any combination thereof.

B. **"Affirmative Express Consent"** means any freely given, specific, informed, and unambiguous indication of an individual'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 such data will be collected, used, or disclosed; (3) the name(s) of any entity that collects the information or to which the information is disclosed; (4) a simple, easily located means for the individual to withdraw consent; (5) any limitations on the individual's ability to withdraw consent; and (6) all other information material to the provision of consent. The Clear and Conspicuous disclosure must be separate from any "privacy policy," "notice of privacy practices," "terms of service," "terms of use," or other similar document.

The following are examples that 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 individual; or (2) obtaining consent through an interface that has the effect of subverting or impairing the individual's autonomy, decision-making, or choice.

C. **"Billing Information"** means any data that enables any person to access a customer's account, such as a credit card, checking, savings, share or similar account, utility bill, mortgage loan account, or debit card.

D. **"Charge," "Charged,"** or **"Charging"** means any attempt to collect money or other consideration from a consumer, including causing Billing Information to be submitted for payment, including against the consumer's credit card, debit card, bank account, telephone bill, or other account.

E. "**Clear(ly) and conspicuous(ly)**" 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 is made in 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 representation that requires the disclosure 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.

F. **"Commitment"** means any representation to consumers, whether located in a privacy or data policy, terms of use, setting, consent flow, user interface or notice, press release, blog post, or otherwise, relating to the collection, storage, maintenance, use, sharing, provision of access to, selling, or deletion of Covered Information.

G. **"Covered Business"** means Defendant and any business that Defendant controls, directly or indirectly.

H. **"Covered Incident"** means any instance in which (1) any United States federal, state, or local law or regulation requires Defendant to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Defendant from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization; or (2) there is a violation of Section I, II, or III of this Order.

I. **"Covered Information"** means information from or about an individual consumer, including: (1) a first and last name; (2) geolocation information sufficient to identify a street name and name of city or town; (3) an email address or other online contact information, such as a user identifier or a screen name; (4) a mobile or other telephone number; (5) photos or videos; (6) a financial account number; (7) credit or debit information; (8) information about or derived from the individual's government-issued identification documents or credentials, such as an image of a driver's license, state identification card, or

passport, or a driver's license number, military identification number, or Social Security number; (9) date of birth; (10) biometric information; (11) static Internet Protocol ("IP") address, user ID, mobile advertising ID, or other persistent identifier that can be used to recognize an individual over time and across different devices, websites, or online services; (12) user account credentials, such as a login name and password (whether plain text, encrypted, hashed, and/or salted); (13) Treatment Information; or (14) any information combined with any of (1) through (13) above.

J. **"Data Product"** means any model, derived data, or other tool developed using Covered Information. Data Product includes but is not limited to any data produced via inference (manual or automated) or predictions, application programming interfaces that incorporate, or are improved or enhanced by, such data, or services or other products that incorporate, or are improved or enhanced by, such data.

K. "**Defendant**" means Cerebral, Inc., d/b/a Cerebral, and its successors and assigns.

L. **"Delete," "Deleted," or "Deletion"** means to remove Covered Information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

M. **"Eligible Customer"** means any consumer from whom Defendant took money for a subscription to or participation in its Negative Option Feature

program after such consumer requested cancellation of their subscription to or participation in the Negative Option Feature program in or before May 2022.

N. **"Health Care Operations"** means: (1) health care quality assessment or improvement activities, including case management and care coordination; (2) health care competency assurance activities, including provider performance evaluation, credentialing, and accreditation; (3) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and legal or regulatory compliance; (4) health care insurance functions, such as underwriting, risk rating, and reinsuring risk; (5) health care business management and administration, including safeguarding Treatment Information, protecting the privacy, confidentiality, security, availability, or integrity of websites and/or other platforms, and enforcing terms of use to the extent they comport with this Order; and (6) general administrative activities, including detecting, preventing, or mitigating fraud or security vulnerabilities. It does not include collecting, using, monetizing (including through the development or use of advertisements, marketing, or other promotional materials), offering for sale, selling, licensing, sharing, transferring, disclosing, or otherwise benefitting from Covered Information collected from consumers for the purposes of serving targeted advertising; enriching data on consumers; or developing, training, refining, improving, or otherwise enhancing any Data Product not used solely for purposes of Treatment.

O. **"Limited Visitor Data"** means (1) static Internet Protocol ("IP") address, user ID, mobile advertising ID, or other persistent identifier that could be used to recognize an individual over time and across different devices, websites, or online services; (2) an email address or other online contact information, such as a user identifier or a screen name; and (3) the particular pages visited by an individual consumer prior to logging into their account and commencing services, *provided that* such pages do not include or otherwise disclose individually identifiable information relating to the past, present, or future physical or mental health or condition(s) of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

P. **"Outside Party"** means any individual or entity other than Defendant or a third party service provider of Defendant that: (1) processes, uses, or receives Covered Information collected by or on behalf of Defendant for and at the direction of the Defendant and no other individual or entity, (2) does not disclose Covered Information, or any individually identifiable information derived from such Covered Information, to any individual or entity other than Defendant 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 (3) does not use Covered Information for any purpose other than performing the services specified in the service provider's contract with Defendant, including (a) a therapist or

prescriber employed by or contracted with Defendant; (b) an employee benefit program that contracts with Defendant for mental health care services on behalf of the employee benefit program's members, employees, and/or clients, provided that before Defendant may disclose any information about any of those members, employees, and/or clients to the employee benefit program, Defendant must require the employee benefit plan to obtain the authorization of the members, employes, and/or clients for such disclosure; or (c) an individual or entity that uses Covered Information only as reasonably necessary to (i) comply with applicable law, regulation, or legal process, (ii) detect, prevent, or mitigate fraud or security vulnerabilities, (iii) 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 (iv) undertake internal research for the technological development and demonstration of Defendant'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.

Q. **"Negative Option Feature"** means, in an offer or agreement to sell or provide any product or service, a provision under which the consumer's silence or failure to take affirmative action to reject a product or service or to cancel the agreement is interpreted by the seller or provider as acceptance or continuing acceptance of the offer.

R. **"Payment"** means activities to obtain payment or reimbursement for the provision or coordination of health care for an individual. It does not include collecting, using, monetizing (including through the development or use of advertisements, marketing, or other promotional materials), offering for sale, selling, licensing, sharing, transferring, disclosing, or otherwise benefitting from Covered Information collected from consumers for the purposes of serving targeted advertising; enriching data on consumers; or developing, training, refining, improving, or otherwise enhancing Algorithms or models not used solely for purposes of Treatment.

S. **"Privacy and Security Risks and Harms"** means the risk to the privacy, confidentiality, security, availability, or integrity of Covered Information that could result in the unauthorized access to, collection, use, retention, misuse, alteration, loss, theft, destruction, or other compromise of such information; and the risk of harm caused, directly or indirectly, by the access to, collection, use, retention, misuse, alteration, loss, theft, destruction, or other compromise of Covered Information, including physical harm, emotional distress or mental health harm, economic harm, reputational harm, relationship harm, discrimination, or harm to an individual's autonomy (*e.g.*, impairing an individual's ability to make his or her own informed decisions, such as through coercion, manipulation, thwarted expectations, or failure to inform the individual of material facts).

T. **"Substance Use Disorder Treatment Product"** means a product for use or marketed for use in the treatment, cure, or prevention of a substance use disorder, such as an opioid use disorder.

U. **"Substance Use Disorder Treatment Service"** means 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, such as an opioid use disorder.

V. **"Telemarketing"** means any plan, program, or campaign which is conducted to induce the purchase of products or services by use of one or more telephones, and which involves a telephone call, whether or not covered by the Telemarketing Sales Rule, 16 C.F.R. part 310.

W. **"Treatment"** means the provision or coordination of health care services or products for an individual. It does not include collecting, using, monetizing (including through the development or use of advertisements, marketing, or other promotional materials), offering for sale, selling, licensing, sharing, transferring, disclosing, or otherwise benefitting from Covered Information collected from consumers for the purposes of serving targeted advertising; enriching data on consumers; or developing, training, refining, improving, or otherwise enhancing Algorithms or models not used solely for purposes of Treatment.

X. **"Treatment Information"** means individually identifiable information relating to the past, present, or future physical or mental health or condition(s) of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, including: (1) medical data, records, and histories, test results, progress notes, the names of health care service providers, or records of consumers' interactions with health care service providers; (2) information concerning the consumer's diagnosis or the provision of health care to the individual; (3) medication, prescription, pharmacy, medical intervention, treatment, and insurance information; (4) information concerning the consumer's use of, creation of an account associated with, or response to a question, questionnaire, or assessment related to, a service or product offered by Defendant or through one of any of Defendant's online properties, services, or mobile applications; (5) information concerning health-related purchases; (6) information concerning the past, present, or future payment for the provision of health care to the consumer; (7) identification numbers or codes for any of the foregoing; or (8) information derived or extrapolated from any of (1)-(7) above (*e.g.*, proxy, derivative, inferred, emergent, or algorithmic data).

ORDER

I. PROHIBITION ON USE OR DISCLOSURE OF COVERED INFORMATION FOR DEFINED ADVERTISING PURPOSES

IT IS ORDERED that:

A. Defendant, and Defendant's officers, agents, and employees who receive actual notice of this Order, whether acting directly or indirectly, are permanently restrained and enjoined from using or disclosing to any third party Covered Information for Defined Advertising Purposes or for any third party's purposes.

B. "Defined Advertising Purposes" means advertising, marketing, promoting, offering, offering for sale, or selling any products or services on, or through websites, mobile applications, or other platforms, including those of a third party, but shall not include the use or disclosure to a third party of Limited Visitor Data for: (i) reporting and analytics related to (a) understanding the user experience on Defendant's websites, apps, or other platforms; (b) Defendant's advertising; and (c) the effectiveness of Defendant's advertising, such as statistical reporting, traffic analysis, and understanding the number of and type of ads served, or conversion measurement; or (ii) communications, services, or products from Defendant requested by a consumer that are sent or provided to the consumer;

provided that the consumer's Limited Visitor Data is not used for targeted advertising and is not used to build a profile about the consumer.

II. AFFIRMATIVE EXPRESS CONSENT

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, and employees, 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 any product or service, are permanently restrained and enjoined from failing to obtain a consumer's Affirmative Express Consent prior to disclosing that consumer's Covered Information to any Outside Party.

III. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, and employees, 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 any Substance Use Disorder Treatment Product, Substance Use Disorder Treatment Service, or any other product or service, are permanently restrained and enjoined from misrepresenting or assisting others in misrepresenting, in any manner, expressly or by implication:

A. The privacy, confidentiality, security, availability, or integrity of any Covered Information;

B. The extent to which they protect the privacy, confidentiality, security, availability, or integrity of any Covered Information;

C. The collection, maintenance, use, disclosure, Deletion, or access permitted or denied to any Covered Information;

D. The extent to which they collect, maintain, use, disclose, Delete, or permit or deny access to any Covered Information;

E. The purposes for which they, or any entity to whom any of them disclose or permit access to Covered Information, collect, maintain, use, disclose, Delete, or permit or deny access to any Covered Information;

F. The extent to which a consumer can maintain privacy and anonymity associated with the consumer's use of products or services offered by Defendant;

G. Their privacy and security measures to prevent unauthorized access to, or use or disclosure of, Covered Information; or

H. Any fact material to consumers concerning any product or service, such as: the total costs; any material restrictions, limitations, or conditions; or any material aspect of its performance, efficacy, nature, or central characteristics.

IV. PROHIBITION AGAINST MISREPRESENTATIONS RELATED TO NEGATIVE OPTIONS

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, and employees, 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 with a Negative Option Feature, are permanently restrained and enjoined from misrepresenting or assisting others in misrepresenting, expressly or by implication:

A. That the consumer can cancel anytime;

B. That the consumer can cancel with no further obligation;

C. Any cost to the consumer to purchase, receive, use, or return the initial product or service;

D. That the consumer will not be Charged for any product or service;

E. That a product or service is offered on a "free," "trial," "sample," "bonus," "gift," "no obligation," "discounted" basis, or words of similar import, denoting or implying the absence of an obligation on the part of the recipient of the offer to affirmatively act in order to avoid Charges, including where a Charge will be assessed pursuant to the offer unless the consumer takes affirmative steps to prevent or stop such a Charge;

F. That the consumer can obtain a product or service for a processing, service, shipping, handling, or administrative fee with no further obligation;

G. Any purpose for which the consumer's Billing Information will be used;

H. The date by which the consumer will incur any obligation or be Charged unless the consumer takes an affirmative action on the Negative Option Feature;

I. That a transaction has been authorized by the consumer;

J. Any material aspect of the nature or terms of a refund, cancellation, exchange, or repurchase policy for the product or service; or

K. Any other material fact.

V. MANDATED PRIVACY AND INFORMATION SECURITY 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 entry of this Order, establish and implement, and thereafter maintain, a comprehensive privacy and information security program ("Program") that protects the privacy, confidentiality, security, availability, and integrity of Covered Information and effectively mitigates Privacy and Security Risks and Harms. To satisfy this requirement, Defendant must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Program mandated in this Section;

B. Provide the written Program required under sub-Section V.A of this Order and any evaluations thereof or adjustments thereto to each Covered Business' Board of Directors (or governing body or, if no such board or body exists, to the senior executive of the Covered Business responsible for the Covered Business' 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 the Chief Executive Officer(s) or, in the event a Chief Executive Officer role does not exist, a similarly-situated executive, to coordinate and be responsible for the Program; and keep the Chief Executive Officer(s) and Board of Directors (or governing body or, if no such board or body exists, to the senior executive of the

Covered Business responsible for the Program) informed of the 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. Conduct and document, at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, a comprehensive risk assessment of the internal and external Privacy and Security Risks and Harms in each area of its operation (*e.g.*, employee and agent training and management; partnerships with third parties to whom the Covered Business has disclosed Covered Information; sharing of Covered Information with third parties; product research, design, and development; advertising; and product marketing and implementation). This assessment must include an evaluation of: (1) each individual product or service feature that collects, uses or shares Covered Information, both on a standalone basis and within the context of the broader product or service that the feature will be supporting or operating (*e.g.*, considering the product or service inclusive of all relevant features); (2) whether existing and fully implemented safeguards effectively mitigate the identified Privacy and Security Risks and Harms for each product or service; (3) whether additional safeguards are available that could better mitigate the identified Privacy and Security Risks and Harms or address any residual unresolved Privacy and Security Risks and Harms; (4) the sufficiency of any proposed consumer notice and, if

necessary, consent; and (5) whether the product or service feature should be deprecated or removed. The Covered Business shall further assess and document the internal and external Privacy and Security Risks and Harms described above as they relate to a Covered Incident promptly following verification or confirmation of such an incident, in any event not to exceed 30 days after the Covered Incident is verified or otherwise confirmed;

E. Design, document, implement, and maintain safeguards that control for the internal and external Privacy and Security Risks and Harms identified in response to sub-Section V.D. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, the severity of the potential Privacy and Security Risks and Harms, and the likelihood that the Privacy and Security Risks and Harms could be realized. The safeguards must also include:

1. Policies, procedures, and standards that describe, at a minimum: (a) how the Covered Business implements each of the safeguards identified in this sub-Section; and (b) how the Covered Business assesses and enforces compliance with the safeguards and any other controls it identifies in its policies, procedures, and standards;

2. Policies, procedures, and technical measures implemented to systematically inventory Covered Information in the Covered Business' control and Delete Covered Information that is no longer necessary;

3. Policies, procedures, and technical measures that prevent the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information inconsistent with the Covered Business's representations to consumers;

4. Policies, procedures, controls, and other requirements that ensure timely identification of, investigation of, disclosure of, and response to Privacy and Security Risks and Harms covered by this Order, timely remediation of Privacy and Security Risks and Harms, and compliance with Sections I-IV of this Order, above;

5. Mandatory, regular privacy and security training for all employees and agents to be conducted when an employee begins employment or takes on a new role with materially different duties or responsibilities, and on at least an annual basis thereafter, updated to address any internal or external Privacy and Security Risks and Harms identified in response to sub-Section V.D and safeguards implemented pursuant to this sub-Section V.E; and which includes, at a minimum, training for each of the Covered Business' employees and agents on the Covered Business' privacy and security policies, standards, and procedures; the requirements of this Order; an introduction to Privacy and Security Risks and Harms and mitigation; and specific role-based training based on the trainee's responsibilities under the Program; and also includes, for developers,

engineers, system or information technology asset administrators, and others that design, implement, and operate the Covered Business' services or products or that are otherwise responsible for the security of Covered Information, training in secure software development principles, including secure engineering and defensive programming concepts; *provided further* that any employee or agent who has not completed annual privacy training within the prior 13 months shall be denied access to Covered Information until such time as they complete the training;

6. Policies, procedures, standards, and technical measures that: (a) control data access for all assets (including databases) containing Covered Information or resources containing proprietary (*i.e.*, non-open source) source code repositories, including, at a minimum: (1) restrictions of inbound connections to those originating from approved IP addresses; (2) requiring connections to be authenticated and encrypted; and (3) periodic audits of account permissions; (b) require and enforce strong passwords or other credentials; (c) prevent the storage of unsecured access keys or other unsecured access credentials; (d) prevent the reuse of known compromised credentials to access Covered Information; and (e) implement automatic password resets for known compromised credentials;

7. Encryption of, at a minimum, all Covered Information, and access credentials used on the Covered Business' systems or information

technology assets, including cloud storage, and data access controls for all systems or information technology assets storing Covered Information, including by, at a minimum, requiring multi-factor authentication methods for all employees, contractors, and affiliates in order to access any assets (including databases) storing Covered Information. Such multi-factor authentication methods for all employees, contractors, and affiliates shall not include telephone or SMS-based authentication methods and must be resistant to phishing attacks. The Covered Business may use widely-adopted industry authentication options that provide at least equivalent security as the multi-factor authentication options required by this sub-Section, if approved in writing by the person responsible for the Program, limiting employee or contractor access to Covered Information to what is needed to perform that employee or contractor's job function;

8. Policies, procedures, standards, and technical measures that assess the risk posed by source code to Covered Information collected or maintained directly or indirectly by the Covered Business, including, at least once every 12 months and promptly (not to exceed 30 days) after a Covered Incident involving a vulnerability related to the Covered Business' source code: (a) software code review; and (b) penetration testing of the Covered Business' software and systems or information technology assets;

9. 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);

10. Policies, procedures, standards, and technical measures that: (a) log and monitor access to repositories of Covered Information; (b) restrict access to any Covered Information to only those employees or agents of the Covered Business who have a business need to access that Covered Information (including, with respect to any health care service provider, providing access only to the Covered Information of consumers to whom that provider personally provides services); and (c) periodically monitor and immediately terminate, within 24 hours, employee and agent access credentials and accounts following inappropriate usage or termination of employment;

11. Requiring an annual self-certification by each third party that obtains or otherwise has access to Covered Information certifying the purpose(s) or use(s) for each type of Covered Information to which it requests or continues to have access, and denying or terminating access to any type of Covered Information that the third party fails to certify unless the third party cures such failure within a reasonable time, not to exceed 30 days;

12. An incident response plan in the form of policies, procedures, standards, and technical measures that ensure a timely identification, investigation, and response to Privacy and Security Risks and Harms covered by this Order and timely remediation thereof. The Covered Business must update this plan to adapt to any material changes affecting compliance with this sub-Section V.E, such as changes to its networks, systems or information technology assets, other assets, or staffing;

13. Policies, procedures, and any other necessary requirements that ensure that (a) any merged or acquired entity, talent, or data, or combination thereof, that becomes part of the Covered Business will comply with the terms of this Order as of the effective date of the merger or Acquisition; (b) any merged or acquired entity, talent, or data, or combination thereof, that becomes an affiliate of the Covered Business will comply with the terms of this Order promptly, and in any event no later than 45 days after the effective date of that affiliate's merger or Acquisition; (c) any entity, talent, or data, or combination thereof, that has stronger privacy or data security protections, policies, and practices than the Covered Business and becomes part of the Covered Business or an affiliate thereof maintains those protections, policies, and practices and continues to honor its prior Commitments to consumers for at least 12 months; and

14. For each product or service, policies and procedures to document internally the decision to collect, use, disclose, or maintain each type of Covered Information. Such documentation should include: (1) the name or names of the person or people who made the decision; (2) for what purpose the type of Covered Information is being collected; (3) the data segmentation controls in place to ensure that the type of Covered Information collected is only used for the particular purpose for which it was collected; (4) the data retention limit set for each type of Covered Information and the technical means for achieving Deletion; (5) the safeguards in place to prevent disclosure or sale of each type of Covered Information in contravention of this Order; and (6) the access controls in place to ensure only authorized employees and agents with a need-to-know have access to each type of Covered Information;

F. Assess, monitor, and test, at least once every 12 months and promptly (not to exceed 30 days) following the resolution of a Covered Incident, the effectiveness of any safeguards put in place pursuant to sub-Section V.E of this Order to address the risks to the privacy, confidentiality, security, availability, or integrity of Covered Information. Such testing and monitoring must include vulnerability testing of each Covered Business' systems websites, apps, and any other platforms once every four months and promptly (not to exceed 30 days) after a Covered Incident. The Covered Business shall modify its Program based on the

results of this assessing, monitoring, and testing at least once every 12 months and promptly (not to exceed 60 days) following the resolution of a Covered Incident;

G. 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

H. Evaluate and adjust the Program in light of any changes to the Covered Business' operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in sub-Section V.D of this Order, and any other circumstances the Covered Business knows or has reason to believe may have a material impact on the effectiveness of the Program or any of its individual safeguards. The Covered Business may make this evaluation and adjustment to its Program at any time, but must, at a minimum, evaluate the Program at least once every 12 months and modify the mandated Program as necessary based on the results.

VI. INDEPENDENT MANDATED PROGRAM ASSESSMENTS

IT IS FURTHER ORDERED that, in connection with compliance with the Section of this Order titled Mandated Privacy and Information Security Program, for any Covered Business that collects, maintains, uses, discloses, or provides access to Covered Information, Defendant must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from one or more qualified, objective, independent third-party professionals ("Assessor(s)"), selected by Defendant, subject to sub-Section VI.B, who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Program; and (3) retains all documents relevant to each Assessment for five years after completion of such Assessment and furnishes 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 by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney client privilege, statutory exemption, or any similar claim;

B. For each Assessment, Defendant must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission ("Associate Director") with the name(s) and affiliation(s) of the person(s) selected to conduct the Assessment, which 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 180 days after the mandated Program has been put in place for the initial Assessment; and (2) each two-year period thereafter for 20 years after entry of this Order, for the biennial Assessments;

D. Each Assessment must: (1) determine whether Defendant has implemented and maintained the Program required by Section V of this Order; (2)

assess the effectiveness of Defendant's implementation and maintenance of each subpart in Section V of this Order; (3) identify any gaps or weaknesses in the Program; (4) identify specific evidence (including 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 sufficient to justify the Assessor's findings; and (5) determine whether Defendant has implemented and maintained the procedures necessary regarding Covered Information to comply with Sections I-V of this Order. To the extent that Defendant revises, updates, or adds one or more safeguards required under Section V.E of this Order in the middle of an Assessment period, the Assessment shall 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. No finding of any Assessment shall rely primarily on assertions or attestations by management of Defendant or any Covered Business. The Assessment shall be signed by the Assessor and shall state that the Assessor conducted an independent review of the mandated Program, and did not rely primarily on assertions or attestations by management of Defendant or any Covered Business;

F. 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, Defendant must submit each 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 Ave. N.W., Washington, DC 20580. The subject line must begin, "FTC v. Cerebral, Inc., FTC File No. 2223067." Each Assessment shall be retained by Defendant and shall be provided to the Commission within 10 days of a request.

VII. COOPERATION WITH ASSESSOR

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, and employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, and each Covered Business, in connection with any Assessment required by the Section of this Order titled Independent Mandated Program Assessments, must:

A. Provide or otherwise make available to the Assessor(s) all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege, including information about all Covered Information in Defendant's custody or control and

all of Defendant's systems or information technology assets so that the Assessor(s) can determine the scope of the Assessment; and

B. Disclose all material facts to each Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's duties pursuant to this Order, or its: (1) determination of whether Defendant has implemented and maintained the Program required by the Section of this Order titled Mandated Privacy and Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Sections V.A-H; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Program.

VIII. ANNUAL CERTIFICATIONS

IT IS FURTHER ORDERED that Defendant must:

A. One year after entry of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior executive of each Covered Business responsible for a Program required by Section V of this Order 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 description of any Covered Incident during the certified period. 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 executive reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, Defendant must submit each annual certification to the Commission and under penalty of perjury as specified in the Section of this Order titled Compliance Reporting.

IX. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Defendant must submit a report within 30 days of Defendant's discovery of a Covered Incident, and subsequently updated every 30 days until the Covered Incident is fully investigated and any remediation efforts are fully implemented, to the Assessor(s) and to the Commission, that includes:

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 of the Covered Incident;

C. A description of each type of information that was affected by the Covered Incident;

D. The number of consumers whose Covered Information was affected by the Covered Incident;

E. The acts that Defendant has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, or any other Privacy and Security Risks and Harms, including a description of any new safeguards that have been implemented in response to the Covered Incident; and

F. A representative copy of any materially different notice sent by Defendant to consumers or to any U.S. federal, state, or local government entity. Defendant must submit each Covered Incident report to the Commission and under penalty of perjury as specified in the Section of this Order titled Compliance Reporting. Within 45 days of Defendant's verification or confirmation of a Covered Incident, Defendant must publish on its websites and apps a public version of each Covered Incident report accessible from its websites' and apps' home screen and maintain each report on its websites and apps for two years.

X. NOTICE TO USERS

IT IS FURTHER ORDERED that, within 14 days of entry of this Order, Defendant must post Clearly and Conspicuously on any screen of its websites, apps, or other platforms where consumers first access or encounter Defendant's products or services, an exact copy of the notice attached hereto as Exhibit A ("Notice"). Defendant must leave this Notice in place for two years after posting it. Defendant must also email the Notice to all consumers that provided Covered Information to it between October 2019 and March 1, 2023, *provided however,* that if Defendant does not have email information for any such consumer, Defendant

must send the Notice to that consumer through its primary means of communicating with that consumer (such as a notification within Defendant's apps). Defendant shall not include with the Notice any other documents, attachments, hyperlinks, or other information.

XI. DATA RETENTION LIMITS AND DELETION OF COVERED INFORMATION AND DATA PRODUCT

IT IS FURTHER ORDERED that Defendant must Delete Covered Information and instruct third parties to Delete Covered Information as follows:

A. Within seven days of entry of this Order, Defendant must document and adhere to a retention schedule for Covered Information in compliance with this Order. Such schedule shall set forth: (1) the purpose or purposes for which each type of Covered Information is collected; (2) the specific business needs for retaining each type of Covered Information; (3) a specific timeframe for Deletion of each type of Covered Information (absent any intervening Deletion requests from consumers) limited to the shortest time necessary to fulfill the purpose for which the Covered Information was collected, and in no instance providing for the indefinite retention of any Covered Information or retention beyond 10 years; and (4) a true and accurate explanation of why the set timeframe for Deletion is the shortest time reasonably necessary for the specific business needs cited.

B. Within 60 days of entry of this Order, Defendant shall Delete all Covered Information in all forms, including hashed or encrypted Covered Information, and any Data Product in its possession, custody, or control that has

not been collected or used for Treatment, Payment, or Health Care Operations, *provided, however, that* Covered Information need not be Deleted to the extent Defendant first obtains the Affirmative Express Consent of the individual for the retention of that Covered Information pursuant to the retention schedule disclosed to the individual, which must be Clearly and Conspicuously disclosed to them in requesting such consent.

C. Within 60 days of entry of this Order, Defendant must provide a Clear and Conspicuous link on the home page or screen and initial login page of Defendant's websites and apps directing individuals to an online form through which they can request access to or the Deletion of their Covered Information. Defendant must respond to every request within 30 days unless the applicable consumer data access and Deletion rights and related procedures prescribed by applicable law provide for an earlier Deletion date. The time period to respond to the request may be extended once by an additional 30 days when reasonably necessary, provided each affected individual is notified in advance of the extension, the reasons for the extension, and the individual's alternatives.

D. Any Covered Information that Defendant is otherwise required to Delete pursuant to this Section may be retained or disclosed to the extent requested by a government agency or otherwise required by law, regulation, court order, or other legal obligation, including as required by rules applicable to the safeguarding of evidence in pending litigation.

E. Additionally, within 30 days of entry of this Order, Defendant must:

1. Identify all third parties that received Covered Information from Defendant in any form, including in hashed or encrypted form;

2. Identify what specific types of Covered Information were disclosed to each third party; and

3. Submit a list disclosing the information identified pursuant to this sub-Section and the methodologies used to obtain that information to the Commission in the same manner specified in the Section of this Order titled Compliance Reporting.

F. Within 60 days of entry of this Order, Defendant must provide a copy of the Complaint in this case and this Order to all third parties identified pursuant to this Section, and instruct those third parties to Delete all Covered Information received from Defendant, directly or indirectly, *provided that* Covered Information need not be deleted pursuant to this sub-Section to the extent that it is used for Treatment, Payment, or Health Care Operations to ensure continuity of care for Defendant's customers. Defendant's instruction to each third party shall include a list of the Covered Information identified pursuant to this Section. Defendant must provide all instructions sent to any third party and all responses received from any of them within 5 days of receipt to the Commission in the same manner specified in the Section of this Order titled Compliance Reporting.

G. As of the date of this Order, Defendant shall not disclose any Covered Information in any form, including hashed or encrypted Covered Information, to any third party until Defendant receives written confirmation from the third party of the third party's receipt of the instructions required by sub-Section F above.

XII. REQUIRED DISCLOSURES RELATING TO NEGATIVE OPTION FEATURE

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, and employees, 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 with a Negative Option Feature, are permanently restrained and enjoined from:

A. Representing directly or indirectly, expressly or by implication, that any product or service that includes a Negative Option Feature is being offered on a free, trial, no obligation, reduced, or discounted basis, without disclosing Clearly and Conspicuously, and immediately adjacent to, any such representation:

1. The extent to which the consumer must take any affirmative action to avoid any Charges: (a) for the offered product or service, (b) of an increased amount after the trial or promotional period ends, and (c) on a recurring basis;

2. The total cost (or range of costs) the consumer will be Charged and, if applicable, the frequency of such Charges unless the consumer timely takes steps to prevent or stop such Charges; and

3. The deadline(s) (by date or frequency) by which the consumer must affirmatively act in order to stop all recurring Charges.

B. Obtaining Billing Information from a consumer for any transaction involving a product or service that includes a Negative Option Feature, without first disclosing Clearly and Conspicuously, and immediately adjacent to where a consumer provides Billing Information:

1. The extent to which the consumer must take affirmative action to avoid any Charges: a) for the offered product or service, b) of an increased amount after the trial or promotional period ends, and c) on a recurring basis;

2. The total cost (or range of costs) the consumer will be Charged, the date the initial Charge will be submitted for payment, and, if applicable, the frequency of such Charges unless the consumer timely takes affirmative steps to prevent or stop such Charges;

3. The deadline(s) (by date or frequency) by which the consumer must affirmatively act in order to stop all recurring Charges;

4. The name of the seller or provider of the product or service and, if the name of the seller or provider will not appear on billing statements, the billing descriptor that will appear on such statements;

5. A description of the product or service;

6. Any Charge or cost for which the consumer is responsible in

connection with the cancellation of an order, any service or the return of any product;

7. The simple cancellation mechanism to stop any recurring Charges, as required by this Order.

C. Failing to send the consumer:

1. Immediately after the consumer's submission of an online order,

written confirmation of the transaction by email. The email must Clearly and Conspicuously disclose all the information required by sub-Section XII.B, and contain a subject line reading "Subscription Confirmation" along with the name of the product or service, and no additional information; or

2. Within 2 days after receipt of the consumer's order by mail or telephone, a written confirmation of the transaction, either by email or first-class mail. The email or letter must Clearly and Conspicuously disclose all the information required by sub-Section XII.B. The subject line of the email must Clearly and Conspicuously state "Subscription Confirmation" along with the name of the product or service, and nothing else. The outside of the envelope must not have any information other than the consumer's address, Defendant's return address, and postage.

XIII. OBTAINING EXPRESS INFORMED CONSENT FOR A NEGATIVE OPTION

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, and employees, 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 with a Negative Option Feature, are permanently restrained and enjoined from using, or assisting others in using, Billing Information to obtain payment from a consumer, unless Defendant first obtains the express informed consent of the consumer to do so. To obtain express informed consent, Defendant must:

A. For all written offers (including over the Internet, such as through a web-based application), obtain consent through a check box, signature, or other substantially similar method, which the consumer must affirmatively select or sign to accept the Negative Option Feature, and no other portion of the offer. Defendant shall disclose Clearly and Conspicuously, and immediately adjacent to such check box, signature, or substantially similar method of affirmative consent, only the following, with no additional information:

1. The extent to which the consumer must take affirmative action to avoid any Charges: (a) for the offered product or service, (b) of an increased amount after the trial or promotional period ends, and (c) on a recurring basis;

2. The total cost (or range of costs) the consumer will be Charged

and, if applicable, the frequency of such Charges unless the consumer timely takes affirmative steps to prevent or stop such Charges; and

3. The deadline(s) (by date or frequency) by which the consumer must affirmatively act in order to stop all recurring Charges.

B. For all oral offers, prior to obtaining any Billing Information from the consumer:

1. Clearly and Conspicuously disclose the information contained in sub-Section B of the Section titled Required Disclosures Relating To Negative Option Feature; and

2. Obtain affirmative unambiguous express oral confirmation that the consumer: (a) consents to being Charged for any product or service, including providing, at a minimum, the last 4 digits of the consumer's account number to be Charged, (b) understands that the transaction includes a Negative Option Feature, and (c) understands the specific affirmative steps the consumer must take to prevent or stop further Charges.

C. For transactions conducted through Telemarketing, Defendant shall maintain for 3 years from the date of each transaction an unedited voice recording of the entire transaction, including the prescribed statements set out in sub-Section XIII.B. Each recording must be retrievable by date and by the consumer's name, telephone number, or Billing Information, and must be provided upon request to the consumer, the consumer's bank, or any law enforcement entity.

XIV. SIMPLE MECHANISM TO CANCEL NEGATIVE OPTION FEATURE

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, and employees, 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 with a Negative Option Feature, are permanently restrained and enjoined from:

A. Failing to provide a simple mechanism for the consumer to: (1) avoid being Charged, or Charged an increased amount, for a product or service and (2) immediately stop any recurring Charge. Such mechanism must:

1. Be easy to find;

2. Be easy to use to stop such Charge; and

3. Not require the consumer to take any action that is objectively unnecessary to cancel, or use a Dark Pattern. A "Dark Pattern" refers to a user interface that has the effect of impeding consumers' expression of preference, manipulating consumers into taking certain action, or otherwise subverting consumers' choice.

B. If any consumers entered into the agreement to purchase a product or service including a Negative Option Feature over the Internet or a mobile phone application, failing to provide the mechanism through the same website, email address or other application.

C. If any consumers entered into the agreement to purchase a product or service including a Negative Option Feature through an oral offer or acceptance, failing to provide such mechanisms through the use of a telephone number and a postal address.

XV. MONETARY JUDGMENTS FOR MONETARY RELIEF AND CIVIL PENALTY

IT IS FURTHER ORDERED that:

A. Judgment in the amount of Five Million, Eighty-Seven Thousand, Two Hundred and Fifty-Two Dollars and Eighty-Nine Cents ($5,087,252.89) is entered in favor of Plaintiff against Defendant as monetary relief.

B. Judgment in the amount of Ten Million Dollars ($10,000,000) is entered in favor of Plaintiff against Defendant as a civil penalty.

C. Defendant is ordered to pay to Plaintiff, by making payment to the Treasurer of the United States, Five Million, Eighty-Seven Thousand, Two Hundred and Fifty-Two Dollars and Eighty-Nine Cents ($5,087,252.89), which, as Defendant stipulates, its undersigned counsel holds in escrow for no purpose other than payment to Plaintiff. Such payment must be made within 7 days of entry of this Order by electronic fund transfer in accordance with instructions provided by a representative of Plaintiff.

D. Defendant is ordered to pay to Plaintiff, by making payment to the Treasurer of the United States, Two Million Dollars ($2,000,000), which, as Defendant stipulates, its undersigned counsel holds in escrow for no purpose other

than payment to Plaintiff. Such payment must be made within 7 days of entry of this Order by electronic fund transfer in accordance with instructions provided by a representative of Plaintiff. Upon such payment, the remainder of the civil penalty judgment is suspended, subject to sub-Section E below.

E. The Commission and Plaintiff's agreement to the suspension of part of the civil penalty judgment in sub-Section B above is expressly premised upon the truthfulness, accuracy, and completeness of Defendant's sworn financial statement and related documents (collectively, "Financial Attestations") submitted to the Commission, including the:

1. Federal Trade Commission Financial Statement of Corporate Defendant and addendum thereto, sworn to by Defendant's Chief Legal Officer, submitted to the FTC on July 26, 2023, and documents listed on the Financial Statement and/or attached thereto;

2. Cerebral, Inc. Consolidated Balance Sheet (Unaudited) for Period Ended June 30, 2023 and Cerebral, Inc. Consolidated Income Statement (Unaudited) for Period Ended June 30, 2023;

3. Consolidated Financial Statements, Cerebral Inc. Including Its Wholly-Owned Subsidiaries and Its Affiliates as of and for the Years Ended December 31, 2022 and 2021 and Independent Auditor's Report;

4. Consolidated Financial Statements, Cerebral Inc. Including Its Wholly-Owned Subsidiaries and Its Affiliates as of and for the Years Ended December 31, 2021 and 2020 and Independent Auditor's Report; and

5. Consolidated Financial Statements, Cerebral Inc. and Affiliates as of and for the Year Ended December 31, 2020 and Independent Auditor's Report.

F. The suspension of the judgment will be lifted as to Defendant if, upon motion by the Commission or Plaintiff, the Court finds that Defendant failed to disclose any material asset, materially misstated the value of any asset, or made any other material misstatement or omission in the financial representations identified above.

G. If the suspension of the judgment is lifted, the judgment becomes immediately due as to Defendant in the amount specified in sub-Section B above (which the parties stipulate only for purposes of this Section represents the amount of the civil penalty for the violations alleged in the Complaint) less any payment previously made pursuant to sub-Section D above, plus interest computed from the date of entry of this Order.

XVI. ADDITIONAL MONETARY PROVISIONS

IT IS FURTHER ORDERED that:

A. Defendant 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, including in a proceeding to enforce its rights to any payment or monetary judgment 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 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. Defendant acknowledges that its Taxpayer Identification Numbers (Social Security Numbers or Employer Identification Numbers), which Defendant must submit 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.

E. All money received by the Commission pursuant to this Order as monetary relief may be deposited into a fund administered by the Commission or its designee to be used for consumer relief, such as 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 such redress is completed, the Commission may apply any remaining money for such related relief (including consumer information remedies) as it determines to be reasonably related to Defendant's practices alleged in the Complaint. Any money not used for relief is to be deposited to the U.S. Treasury as an additional civil penalty. Defendant has no right to challenge any actions the Commission or its representatives may take pursuant to this sub-Section or Section XVII.

XVII. INDEPENDENT REDRESS ADMINISTRATOR

IT IS FURTHER ORDERED that, if a representative of the Commission decides that redress to consumers is practicable, 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 Defendant.

B. Within 7 days of receipt of a written notification from a representative of the Commission that redress to consumers is practicable, Defendant must provide the Administrator with all information necessary to identify all Eligible Customers and all information necessary for the efficient administration of consumer redress to those Eligible Customers. Defendant 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, Defendant 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 Eligible Customer information shall be directed solely to the Administrator.

C. The Administrator shall be responsible for reviewing, assessing, and evaluating the Eligible 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 Defendant 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 Eligible Customer information with the Commission.

2. Within 45 days of days of receipt of customer information provided by Defendant to administer consumer redress as determined by the Commission, the Administrator shall confirm in writing that it has a complete list of Eligible 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 Eligible Customer information they receive from the Administrator, and the Administrator must contractually require service providers to implement and maintain safeguards for such 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 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 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. Defendant must fully cooperate with and assist the Administrator. That cooperation and assistance must include 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 Defendant.

E. Defendant 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 Section XV of this Order shall be used to pay for the Administrator or any of its associated costs or fees.

XVIII. ORDER ACKNOWLEDGMENTS

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

A. Defendant, within 7 days of entry 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 entry of this Order, for all Covered Businesses and any business that Defendant, individually or collectively with any other Defendant, is the majority owner or controls directly or indirectly, Defendant must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees and agents having managerial responsibilities for privacy or data security; (3) all employees and agents having responsibilities for the promotion or sale of health-related products or services, or products or services with a Negative Option Feature; (4) any business entity resulting from any change in structure as set forth in the Section titled Compliance Reporting; and (5) each Covered Business. Delivery must occur within 7 days of entry 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 a Defendant delivered a copy of this Order, that Defendant must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

XIX. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that Defendant make timely submissions to the Commission:

A. One year after entry of this Order, Defendant must submit a compliance report, sworn under penalty of perjury. In this report, Defendant must:

1. Identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission and Plaintiff may use to communicate with Defendant;

2. Identify all of Defendant's businesses (including any Covered Business) by all of their names, telephone numbers, and physical, postal, email, and Internet addresses;

3. Describe the activities of each business, including the products and services offered, the means of advertising, marketing, and sales, including any marketing with a Negative Option Feature, describe in detail how Defendant's privacy policies, procedures, and practices and data security policies, procedures, and practices have changed since March 1, 2023, and describe the involvement of any other defendant;

4. Describe in detail whether and how Defendant is in compliance with each Section of this Order; and

5. Provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission.

B. For 20 years after entry of this Order, Defendant must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following:

1. Any designated point of contact; or

2. The structure of Defendant, any Covered Business, or any entity that Defendant has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, 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. Defendant must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Defendant 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: "FTC v. Cerebral, Inc., File No. 2223067."

XX. RECORDKEEPING

IT IS FURTHER ORDERED that Defendant must create certain records for 20 years after entry of the Order, and retain each such record for 5 years. Specifically, Defendant, in connection with the marketing of any health services or products or any service or product with a Negative Option Feature, must create and retain the following records:

A. Accounting records showing the revenues from all products or services sold;

B. Personnel records showing, for each person providing services, 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. Records of all consumer complaints and refund requests, whether received directly or indirectly, such as through a third party, and any response;

D. All records necessary to demonstrate full compliance with each Section of this Order, including all submissions to the Commission; and

E. A copy of each unique advertisement or other marketing material offering a service or product with a Negative Option feature, or containing a

privacy or data security Commitment, including any representation relating to the handling or treatment (such as Deletion) of Covered Information.

XXI. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Defendant's compliance with this Order and any failure to transfer any assets as required by this Order:

A. Within 14 days of receipt of a written request from a representative of the Commission or Plaintiff, Defendant must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce documents for inspection and copying. The Commission and Plaintiff are also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, the Commission and Plaintiff are authorized to communicate directly with Defendant. Defendant must permit representatives of the Commission and Plaintiff to interview any employee or other person affiliated with any Defendant who has agreed to such an interview. The person interviewed may have counsel present.

C. The Commission and Plaintiff may use all other lawful means, including posing, through its representatives as consumers, suppliers, or other

individuals or entities, to Defendant or any individual or entity affiliated with Defendant, 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 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XXII. COOPERATION

IT IS FURTHER ORDERED that Defendant Cerebral, Inc. must fully cooperate with representatives of Plaintiff and the Commission in this case and in any investigation related to or associated with the transactions or the occurrences that are the subject of the Complaint. Defendant must provide truthful and complete information, evidence, and testimony. Defendant must cause its officers, employees, representatives, or agents to appear for interviews, discovery, hearings, trials, and any other proceedings that a Plaintiff or Commission representative may reasonably request upon 5 days' written notice, or other reasonable notice, at such places and times as a Plaintiff or Commission representative may designate, without the service of a subpoena.

XXIII. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

DONE AND ORDERED in Chambers at Miami, Florida this ___ day of April, 2024.

_____

UNITED STATES DISTRICT JUDGE

individuals or entities, to Defendant or any individual or entity affiliated with Defendant, 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 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XXII. COOPERATION

IT IS FURTHER ORDERED that Defendant Cerebral, Inc. must fully cooperate with representatives of Plaintiff and the Commission in this case and in any investigation related to or associated with the transactions or the occurrences that are the subject of the Complaint. Defendant must provide truthful and complete information, evidence, and testimony. Defendant must cause its officers, employees, representatives, or agents to appear for interviews, discovery, hearings, trials, and any other proceedings that a Plaintiff or Commission representative may reasonably request upon 5 days' written notice, or other reasonable notice, at such places and times as a Plaintiff or Commission representative may designate, without the service of a subpoena.

XXIII. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

DONE AND ORDERED in Chambers at Miami, Florida this ___ day of April, 2024.

_____

UNITED STATES DISTRICT JUDGE

SO STIPULATED AND AGREED:

FOR PLAINTIFF, THE UNITED STATES FOR OF AMERICA:

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division

ARUN G. RAO
Deputy Assistant Attorney General

AMANDA LISKAMM
Director
Consumer Protection Branch

LISA K. HSIAO
Senior Deputy Director Civil Litigation

RACHAEL L. DOUD
Assistant Director

By: *[/s/ Shana C. Priore](#)*
JOSHUA A. FOWKES
SHANA C. PRIORE
FRANCISCO L. UNGER
Trial Attorneys
Consumer Protection Branch
U.S. Department of Justice
450 5th Street, N.W. Suite 6400-South
Washington, D.C. 20044
202-532-4218 (Fowkes)
202-598-8182 (Priore)
202-742-7111 (Unger)
Fax: 202-514-8742
Joshua.A.Fowkes@usdoj.gov
Shana.C.Priore2@usdoj.gov
Francisco.L.Unger@usdoj.gov

MARKENZY LAPOINTE
United States Attorney
Southern District of Florida

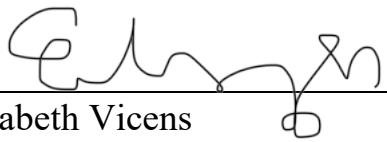
Rosaline Chan
Assistant United States Attorney
99 NE 4th St.
Miami, FL 33132
305-961-9335
Rosaline.Chan@usdoj.gov

FOR THE FEDERAL TRADE COMMISSION:

/s/ Joshua S. Millard
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 (Fax)
jmillard@ftc.gov
cerickson@ftc.gov

Date: February 27, 2024

FOR DEFENDANT, CEREBRAL, INC.:



Date: 02/06/2024

Elizabeth Vicens
Cleary Gottlieb Steen & Hamilton LLP
One Liberty Plaza
New York, NY 10006-1470
212-225-2524
evicens@cgsh.com

Tom Bednar
Cleary Gottlieb Steen & Hamilton LLP
2112 Pennsylvania Ave., N.W.
Washington, D.C. 20037
202-974-1836
tbednar@cgsh.com

COUNSEL FOR CEREBRAL, INC.

David Mou

Date: 2024-02-06

DR. DAVID MOU AS CEO
OF CEREBRAL, INC.

EXHIBIT A

[To appear with the Cerebral, Inc. logo]

Website and Mobile Application Notice

Between October 2019 and [date], we shared the personal of information of consumers visiting our website and apps with other companies without their permission. Specifically, we shared details about consumers (including contact information, birthdates, IP addresses, and other demographic information); any intake questionnaire responses they provided (including selected services and other personal health information); location information; and subscription or other treatment information (including appointment dates, clinical information, and insurance and pharmacy information) with approximately two-dozen outside firms, including social media firms such as Facebook / Meta and Tik Tok, and other businesses such as Google.

The Federal Trade Commission says we broke the law by sharing this information without users' permission. To resolve the case with the FTC,

- We'll delete all personal and health information we collected or used without consumers' permission for any purpose other than providing health care, unless consumers consent to our retaining that information for health care purposes. And we'll tell other firms to delete that information, too.
- We won't share any health information with any company unless we get our users' permission.
- We'll put in place a comprehensive privacy and information security program to protect consumers' information. A third party will audit our program to make sure we are protecting our users' information. These audits will happen every two years for 20 years.

If you have any questions, you can email us at [email]@cerebral.com.

To learn more about the settlement, go to ftc.gov and search for "Cerebral, Inc.".

Read the FTC's Does your health app protect your sensitive info? to learn more about protecting your health privacy.

Notice to Consumers

Between October 2019 and [date], you used Cerebral, Inc.'s website and/or app. During that time, we shared your information with other companies without your

permission. Specifically, we shared details about you (including contact information, birthdates, IP addresses, and other demographic information); any intake questionnaire responses you provided (including selected services and other personal health information); your location information; and any subscription or other treatment information for you (including appointment dates, clinical information, and insurance and pharmacy information) with approximately two-dozen outside firms, including social media firms such as Facebook / Meta and Tik Tok, and other businesses such as Google.

The Federal Trade Commission says we broke the law by sharing this information without your permission. To resolve the case with the FTC,

- We'll delete all personal and health information we collected or used without consumers' permission for any purpose other than providing health care, unless consumers consent to our retaining that information for health care purposes. And we'll tell other firms to delete that information, too.
- We won't share any health information with any company unless we get our users' permission.
- We'll put in place a comprehensive privacy and information security program to protect consumers' information. A third party will audit our program to make sure we are protecting our users' information. These audits will happen every two years for 20 years.

If you have any questions, you can email us at [email]@cerebral.com.

To learn more about the settlement, go to ftc.gov and search for "Cerebral, Inc.".

Read the FTC's Does your health app protect your sensitive info? to learn more about protecting your health privacy.