UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, United States Department of Justice Consumer Protection Branch 450 5th St. NW, Suite 6400, Washington, DC 20001, **Plaintiff**, v. **MONUMENT, INC.**, a Delaware limited liability company, 350 7th Ave. New York, NY 10001, **Defendant**.	**Case No.** **[PROPOSED] STIPULATED ORDER FOR PERMANENT INJUNCTION, CIVIL PENALTY JUDGMENT, AND OTHER RELIEF**

Plaintiff, the United States of America, acting upon notification and referral to the Attorney General by the Federal Trade Commission ("Commission"), filed its Complaint for Civil Penalties, Permanent Injunction, and Other Relief ("Complaint") in this matter, pursuant to Sections 13(b), 16(a)(1), and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 53(b), 56(a)(1), and 57b, and Section 8023 of the Opioid Addiction Recovery Fraud Prevention Act of 2018, 15 U.S.C. § 45d ("OARFPA"). Defendant has waived service of the summons and the Complaint. Plaintiff and Defendant stipulate to the entry of this Stipulated Order for Permanent Injunction, 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 Defendant participated in deceptive and unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, in connection with Defendant's failure to employ reasonable measures to prevent the disclosure of consumers' health information via tracking technologies to third parties for advertising and the third parties' own purposes; failure to obtain consumers' affirmative express consent before disclosing their health information to third parties; misrepresentations that Defendant would not disclose consumers' health information to third parties without those consumers' knowledge or consent; and misrepresentations that Defendant was compliant with the Health Insurance Portability and Accountability Act ("HIPAA"). The Complaint also charges that Defendant's deceptive acts or practices in connection with Defendant's alcohol addiction treatment service violated Section 8023 of OARFPA.

3. Defendant neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this 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 and Plaintiff waive all rights to appeal or to otherwise challenge or contest the validity of this Order.

DEFINITIONS

For purposes of this Order, the following definitions apply:

A. "**Affirmative Express Consent**" means any freely given, specific, informed, and unambiguous indication of an individual consumer's wishes demonstrating agreement by the

consumer, such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the consumer of:

1. the categories of information that will be collected;
2. the specific purpose(s) for which the information is being collected, used, or disclosed;
3. the names or categories of Third Parties (e.g., "analytics partners" or "advertising partners") collecting the information, or to whom the information is disclosed, provided that if Defendant discloses the categories of Third Parties, the disclosure shall include a hyperlink to a separate page listing the names of the Third Parties;
4. a simple, easily located means by which the consumer can withdraw consent; and
5. any limitations on the consumer's ability to withdraw consent.

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

The following do not constitute Affirmative Express Consent:

1. Inferring consent from the hovering over, muting, pausing, or closing of a given piece of content by the consumer; or
2. Obtaining consent through a user interface that has the effect of subverting or impairing user autonomy, decision-making, or choice.

B. "**Clear(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.

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

D. "**Covered Incident**" means any instance of a violation of Section I, II, or III of this Order.

E. "**Covered Information**" means information from or about an individual consumer, including:

1. a first and last name;
2. a physical address, including street name and name of city or town;
3. geolocation information sufficient to identify street name and name of a city or town;
4. an email address or other online contact information, such as a user identifier or a screen name;
5. a telephone number;
6. a government-issued identification number, such as a driver's license, military identification, passport, Social Security number, or other personal identification number;
7. financial institution account number;
8. credit or debit card information;
9. data that depicts or describes the physical or biological traits of an

identified or identifiable person, including depictions, descriptions, recordings, or copies of an individual's facial or other physical features, finger or handprints, voice, genetics, or characteristic movements or gestures;

10. a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, advertising ID, processor serial number, or any other persistent identifier that can be used to recognize a user over time and/or across difference devices, websites, or online services;
11. Health Information; or
12. any individually identifiable information combined with any of (1) through (11) above.

Provided however that "Covered Information" does not include Protected Health Information, or information treated in accordance with the safeguards set forth in the HIPAA Privacy Rule, 45 C.R.F. Parts 160 and 164 and the HIPAA Security Rule, 45 C.F.R. Parts 160 and Subparts A and C of Part 164.

F. "**Covered User**" means any individual consumer who: (1) created an account with Defendant before December 29, 2022; and (2) to whom Defendant did not send a breach notification on or about March 23, 2023.

G. "**Defendant**" means Monument, Inc., doing business as Monument Health Services, its successors and assigns, and Tempest, Inc., and its successors and assigns.

H. "**Delete**," "**Deleted**," or "**Deletion**" means to remove Covered Information such that it is not maintained in retrievable form and cannot be retrieved through physical or technical means.

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

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

J. "**Personal Information**" means information from or about an individual consumer, including:

1. a first and last name;
2. a physical address, including street name and name of city or town;
3. geolocation information sufficient to identify street name and name of a

city or town;

4. an email address or other online contact information, such as a user identifier or a screen name;
5. a telephone number;
6. a government-issued identification number, such as a driver's license, military identification, passport, Social Security number, or other personal identification number;
7. financial institution account number;
8. credit or debit card information;
9. data that depicts or describes the physical or biological traits of an identified or identifiable person, including depictions, descriptions, recordings, or copies of an individual's facial or other physical features, finger or handprints, voice, genetics, or characteristic movements or gestures;
10. a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, processor serial number, or any other persistent identifier that can be used to recognize a user over time and/or across difference devices, websites, or online services;
11. Health Information; or
12. any individually identifiable information combined with any of (1) through (11) above.

K. "**Protected Health Information**" means individually identifiable health information:

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

   (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.

2. Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years.

L. "**Third Party**" means any individual or entity other than:

1. Defendant;
2. a service provider of Defendant that:
   a. 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,
   b. 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
   c. does not use Covered Information for any purpose other than

performing the services specified in the service provider's contract with Defendant;

3. a therapist, counselor, physician or other health-care provider employed by or contracted with Defendant;
4. an insurer, clearinghouse, or any other party to whom disclosure of Covered Information is necessary to submit or process an insurance claim; or
5. any entity (including a service provider) that uses Covered Information only as reasonably necessary to:
    a. comply with applicable law, regulation, or legal process;
    b. detect, prevent, or mitigate fraud or security vulnerabilities;
    c. debug to identify and repair errors that impair existing intended functionality provided that any such use is reasonably necessary and proportionate to achieve the purpose for which the Covered Information was collected or processed; or
    d. undertake internal research for the technological development and demonstration of 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.

ORDER

I. BAN ON DISCLOSURE OF HEALTH INFORMATION FOR ADVERTISING PURPOSES

IT IS ORDERED that:

A. Defendant, Defendant's officers, agents, employees, and attorneys who receive actual notice of this Order, whether directly or indirectly, are permanently restrained and enjoined from disclosing Health Information to Third Parties for Advertising Purposes.

B. For purposes of this Section, "Advertising Purposes" means advertising, marketing, promoting, offering, offering for sale, or selling any products or services on, or through Third Party websites, mobile applications, or services. Advertising Purposes shall not include: (i) reporting and analytics related to understanding advertising and advertising effectiveness, such as statistical reporting, traffic analysis, understanding the number of and type of ads served, or conversion measurement; or (ii) communications, services, or products requested by a consumer that are sent or provided to the consumer; or (iii) contextual advertising, meaning non-personalized advertising shown as part of a consumer's current interaction with Defendant's website or mobile applications, provided that the consumer's Covered Information is not disclosed to another Third Party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interactions with Defendant's websites or mobile application.

II. REQUIREMENT TO OBTAIN AFFIRMATIVE EXPRESS CONSENT FOR ANY OTHER DISCLOSURE OF HEALTH INFORMATION

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any

product or service, prior to disclosing any consumer's Health Information to any Third Party, must obtain the relevant consumer's Affirmative Express Consent.

III. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with promoting or offering for sale any good or service are permanently restrained and enjoined from misrepresenting, expressly or by implication:

A. the extent to which Defendant collects, maintains, uses, discloses, Deletes, or permits or denies access to any Personal Information, or the extent to which Defendant protects the privacy, security, availability, confidentiality, or integrity of any Personal Information;

B. the purpose(s) for which Defendant, or any entity to whom Defendant discloses or permits access to Personal Information, collects, maintains, uses, discloses, or permits access to any Personal Information;

C. the extent to which a consumer can maintain privacy, confidentiality, or anonymity when visiting or using any online properties, services, or mobile applications associated with Defendant; and

D. the extent to which Defendant is a HIPAA-covered entity, and the extent to which Defendant's privacy and information practices, policies, and procedures comply with HIPAA.

IV. DATA DELETION

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with promoting or offering for sale any good or service, must:

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

   1. identify all Third Parties that accessed, received, or acquired Covered Information from Defendant in any form, including hashed or encrypted Covered Information, without a consumer's Affirmative Express Consent;
   2. identify what Covered Information was disclosed to each Third Party identified in sub-Section IV.A.1;
   3. submit a list of the information identified in sub-Sections IV.A.1-2 and the methodologies used to identify the information in sub-Sections IV.A.1-2 to the FTC's Division of Enforcement, Bureau of Consumer Protection, in accordance with Provision XIV.E; and

B. within 90 days after the effective date of this Order, provide a copy of the Complaint and Order to all Third Parties identified in sub-Section IV.A.1, and instruct those Third Parties to Delete all Covered Information accessed, received, or acquired from Defendant. Defendant's instruction to each such Third Party shall include a list of the Covered Information identified in sub-Section IV.A.2 and shall demand written confirmation from each such Third Party that it has Deleted such Covered Information. Defendant must provide all instructions sent to the Third Parties to the FTC's Division of Enforcement, Bureau of Consumer Protection, in accordance with Provision XIV.E;

C. as of the issuance of this Order Defendant shall not disclose any Covered Information in any form, including hashed or encrypted Covered Information, to any Third Party identified in sub-Section IV.A.1 until Defendant confirms each Third Party's receipt of the instructions required by sub-Section IV.B. This sub-Section is subject to the prohibitions set forth in Section I. Defendant must provide all receipts of confirmation and any responses from Third Parties within five (5) days of receipt to the FTC's Division of Enforcement, Bureau of Consumer Protection, in accordance with Provision XIV.E.

V. NOTICE

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

VI. MANDATED PRIVACY PROGRAM

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

A. document in writing the content, implementation, and maintenance of the Privacy Program;

B. provide the written program and any evaluations thereof or updates thereto to the Covered Business's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of the Covered Business responsible for the Covered Business's Privacy Program at least once every 12 months and promptly (not to exceed 30 days) after a Covered Incident;

C. designate a qualified employee or employees, who report(s) directly to an executive, such as the Chief Executive Officer, Chief Compliance Officer, or Chief Legal Officer, to coordinate and be responsible for the Privacy Program; and keep the executive and the Board of Directors informed of the Privacy Program, including all actions and procedures implemented to comply with the requirements of this Order, and any actions and procedures to be implemented to ensure continued compliance with this Order;

D. assess and document, at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, internal and external risks in each area of the Covered Business's operations to the privacy, security, availability, confidentiality, and integrity of Covered Information that could result in the unauthorized access, collection, use, destruction, or disclosure of, or provision of access to, Covered Information;

E. design, implement, maintain, and document safeguards that control for the internal and external risks to the privacy, security, availability, confidentiality, and integrity of Covered Information identified by the Covered Business in

response to sub-Section VI.D. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, Deletion, disclosure of, or provision of access to, the Covered Information. Such safeguards must also include:

1. policies, procedures, and technical measures to systematically inventory Covered Information in the Covered Business's control and Delete Covered Information that is no longer reasonably necessary and in accordance with applicable retention laws and regulations;
2. policies, procedures, and technical measures to prevent the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information inconsistent with the Covered Business's representations to consumers;
3. audits, assessments, and reviews of the contracts, privacy policies, and terms of service associated with any Third Party to which the Covered Business discloses, or provides access to, Covered Information;
4. policies and technical measures that limit employee and contractor access to Covered Information to only those employees and contractors with a legitimate business need to access such Covered Information;
5. mandatory privacy training programs for all employees with access to Covered Information in connection with the Covered Business on at least an annual basis, with such training covering any internal or external risks identified by Defendant in sub-Section VI.D the safeguards implemented

pursuant to sub-Section VI.E, and the requirements of this Order;

6. a data retention policy that, at a minimum, includes:
    i. a retention schedule that limits the retention of Covered Information to the shortest time necessary to fulfill the purpose for which the Covered Information was collected; provided, however, that such Covered Information need not be Deleted, and may be disclosed, to the extent requested by a government agency or required by law, regulation, or court order; and
    ii. a requirement that Defendant documents, adheres to, and makes publicly available on its terms of service/use a retention schedule for Covered Information, setting forth: (1) the purposes for which the Covered Information is collected; (2) the specific business need for retaining each type of Covered Information; and (3) a set timeframe in accordance with applicable laws and regulations for Deletion of each type of Covered Information (absent any intervening Deletion requests from consumers) that precludes indefinite retention of any Covered Information;
7. audits, assessments, reviews, or testing of each mechanism by which the Covered Business discloses Covered Information to a Third Party or provides a Third Party with access to Covered Information (including but not limited to web beacons, pixels, and Software Development Kits); and
8. for each product or service offered by any Covered Business, Clearly and Conspicuously disclose the categories of Covered Information collected

from consumers, the purposes for the collection of each category of Covered Information, and any transfer of Covered Information to a Third Party. For each such transfer of Covered Information, the disclosure must, at a minimum, include: (a) the specific categories of Covered Information transferred; (b) the identity of each Third Party receiving the transfer; (c) the purposes for which the Covered Business transferred the Covered Information to each Third Party; (d) the purposes for which each Third Party receiving the Covered Information may use the Covered Information, including but not limited to the purposes for which the Third Party reserves the right to use such Covered Information; and (e) whether each Third Party receiving the Covered Information reserves the right to transfer the Covered Information to other entities or individuals.

F. assess, at least once every 12 months, and promptly (not to exceed 30 days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, availability, confidentiality, and integrity of Covered Information, and modify the Privacy Program based on the results;

G. test and monitor the effectiveness of the safeguards at least once every 12 months, and promptly (not to exceed 30 days) following a Covered Incident, and modify the Privacy Policy based on the results;

H. select and retain service providers capable of safeguarding Covered Information they receive from the Covered Business, and contractually require service providers to implement and maintain safeguards for Covered Information; and

I. evaluate and adjust the Privacy Program in light of any material changes to the Covered Business's operations or business arrangements, the results of the testing and monitoring required by sub-Section VI.G, a Covered Incident, and any other circumstances that the Covered Business knows or has reason to believe may have a material impact on the effectiveness of the Privacy Program or any of its individual safeguards (including but not limited to new or more efficient technological or operational methods to control for the risks identified in sub-Section VI.D). The Covered Business may make this evaluation and adjustment to the Privacy Program at any time, but must, at a minimum, evaluate the Privacy Program at least once every 12 months and modify the Privacy Program as necessary based on the results.

VII. PRIVACY ASSESSMENTS BY A THIRD-PARTY ASSESSOR

IT IS FURTHER ORDERED that, in connection with its compliance with Section VI, 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 a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Privacy Program; (3) retains all documents relevant to each Assessment for 5 years after completion of such Assessment; and (4) will provide such documents to the Commission within 10 days of receipt of a written request from a representative of the Commission. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-

client privilege, statutory exemption, or any similar claim. The Assessor must have a minimum of 3 years of experience in the field of privacy and data protection.

B. For each Assessment, Defendant must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in his or her sole discretion.

C. The reporting period for the Assessments must cover: (1) the first year after the issuance date of the Order for the initial Assessment; and (2) each 2-year period thereafter for 20 years after the issuance date of the Order for the biennial Assessments.

D. Each Assessment must, for the entire assessment period:

1. determine whether Defendant has implemented and maintained the Privacy Program required by Section VI;
2. assess the effectiveness of Defendant's implementation and maintenance of sub-Sections VI.A-I;
3. identify any gaps or weaknesses in the Privacy Program, or instances of material noncompliance with, sub-Sections VI.A-I;
4. address the status of gaps or weaknesses in the Privacy Program, as well as any instances of material non-compliance with sub-Sections VI.A-I, that were identified in any prior Assessment required by this Order; and
5. identify specific evidence (including, but not limited to, documents

reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise of Defendant's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely solely on assertions or attestations by Defendant, Defendant's management, or a Covered Business's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Privacy Program and did not rely solely on assertions or attestations by Defendant, Defendant's management, or a Covered Business's management, and state the number of hours that each member of the Assessor's assessment team worked on the Assessment. To the extent a Covered Business revises, updates, or adds one or more safeguards required under sub-Section VI.E in the middle of an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Defendant must submit the initial Assessment to the Commission within 10 days after the Assessment has been completed via email to the FTC's Division of Enforcement, Bureau of Consumer

Protection, in accordance with Provision XIV.E. All subsequent biennial Assessments must be retained by Defendant until the Order is terminated and provided to the Associate Director for Enforcement within 10 days of request.

VIII. COOPERATION WITH ASSESSOR

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

A. provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

B. provide or otherwise make available to the Assessor information about all Covered Information in Defendant's custody or control so that the Assessor can determine the scope of the Assessment; and

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

IX. ANNUAL CERTIFICATION

IT IS FURTHER ORDERED that Defendant must:

A. one year after the issuance date of this Order, and each year thereafter for 10 years, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of each

Covered Business that: (1) the Covered Business has established, implemented, and maintained the requirements of this Order; (2) the Covered Business is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of any Covered Incident. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

B. unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to the FTC's Division of Enforcement, Bureau of Consumer Protection, in accordance with Provision XIV.E.

X. COVERED INCIDENT REPORTS

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

A. the date, estimated date, or estimated date range when the Covered Incident occurred;

B. a description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;

C. the number of consumers whose information was affected;

D. the acts that Defendant has taken to date to remediate the Covered Incident; protect Covered Information from further disclosure, exposure, or access; and protect affected individuals from identity theft or other harm that may result from

the Covered Incident; and

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

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to the FTC's Division of Enforcement, Bureau of Consumer Protection, in accordance with Provision XIV.E.

XI. MONETARY JUDGMENT FOR CIVIL PENALTY AND SUSPENSION

IT IS FURTHER ORDERED that:

A. Judgment in the amount of Two Million and Five Hundred Thousand Dollars ($2,500,000) is entered in favor of Plaintiff against Defendant, as a civil penalty.

B. The judgment is suspended, subject to the sub-Sections below.

C. Plaintiff's agreement to the suspension of the judgment is expressly premised upon the truthfulness, accuracy, and completeness of Defendant's sworn financial statements and related documents (collectively, "Financial Representations") submitted to the Commission, namely:

1. the Financial Statement of Defendant signed by Michael Russell, Chief Executive Officer, on October 12, 2023, including the attachments; and
2. the additional documentation submitted by Defendant via counsel to Commission counsel on October 12, 2023, attaching the above-referenced Financial Statement of Defendant, 2020 Tax Return of Defendant, 2021 Tax Return of Defendant, and Consolidated Financial Statements of Defendant as of October 12, 2023 (including a Profit and Loss Statement, Balance Sheet, and Statement of Cash Flows since January 2020).

3. the additional documentation submitted by email from Defendant via counsel to Commission counsel dated October 30, 2023, attaching the 2022 Tax Return of Defendant.
4. the additional documentation submitted by Defendant via counsel to Commission counsel dated November 20, 2023.

D. The suspension of the judgment will be lifted as to Defendant if, upon motion by the 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.

E. If the suspension of the judgment is lifted, the judgment becomes immediately due as to Defendant in the amount specified in sub-Section A 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 this Section, plus interest computed from the date of entry of this Order.

XII. 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 Plaintiff or the Commission, including in a proceeding to enforce its rights to any payment or monetary judgment pursuant to this Order, such as a nondischargeable 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 agrees that the judgment represents a civil penalty owed to the government of the United States, is not compensation for actual pecuniary loss, and, therefore, it is not subject to discharge under the Bankruptcy Code pursuant to 11 U.S.C. § 523(a)(7).

E. Defendant acknowledges that its Taxpayer Identification Numbers (Social Security Numbers or Employer Identification Numbers), which Defendant previously submitted to the Commission, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. §7701.

XIII. 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 3 years after entry of this Order, Defendant must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in Section XIV. 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 Defendant delivered a copy of this Order, Defendant must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

XIV. 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, which does the following: (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 by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describe the activities of each business; (4) describe in detail whether and how Defendant is in compliance with each Provision 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 10 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 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 such 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: United States v. Monument, Inc. [X number].

XV. RECORDKEEPING

IT IS FURTHER ORDERED that Defendant must create certain records for 10 years after entry of the Order, and retain each such record for 5 years. Specifically, Defendant must create and retain the following records:

A. accounting records showing the revenues from all goods 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;

and

C. all records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission.

XVI. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Defendant's compliance with this Order, including the financial representations upon which the judgment was suspended:

A. Within 14 days of receipt of a written request from a representative of the Commission, 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 their 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 or Plaintiff's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XVII. 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.

SO ORDERED this ___ day of _____, 2024.

_____
UNITED STATES DISTRICT JUDGE

SO STIPULATED AND AGREED:

FOR PLAINTIFF THE UNITED STATES OF AMERICA:

BRIAN BOYNTON
Assistant Attorney General, Civil Division
U.S. DEPARTMENT OF JUSTICE

AMANDA N. LISKAMM
Director, Consumer Protection Branch

LISA K. HSIAO
Senior Deputy Director

ZACHARY A. DIETERT
Assistant Director

Richard S. Greene IV

Date: 4/11/24

RICHARD S. GREENE
Senior Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
P.O. Box 386
Washington, DC 20044
Phone: 202-305-3827
Email: Richard.s.greene.iv@usdoj.gov

FEDERAL TRADE COMMISSION

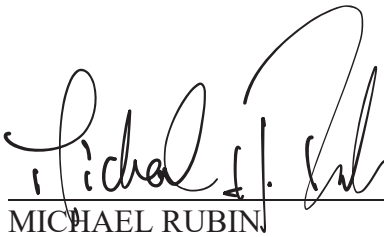
/s/ Elisa Jillson

ELISA JILLSON (DC Bar No. 989763)
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-3001 (voice); -3062 (fax)
Email: ejillson@ftc.gov

/s/ Robin Rosen Spector

ROBIN ROSEN SPECTOR (DC Bar No. 449324)
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-3740 (voice); -3062 (fax)
Email: rspector@ftc.gov

FOR DEFENDANT:



Date: Feb. 16, 2024

MICHAEL RUBIN
Latham & Watkins LLP
505 Montgomery Street
Suite 2000
San Francisco, CA 94111-6538

DocuSigned by:
Michael Russell
988808081009496...

Date: 16 February 2024

MONUMENT, INC.
BY MICHAEL RUSSELL, CEO

Exhibit A

Notice to Covered Users

[Subject: The United States Department of Justice and the Federal Trade Commission Allege That We Shared Information About You Without Your Permission]

[To appear with the Monument logo]

Hello,

We are contacting you because you used Monument's services or created an account for one of these services before December 29, 2022. When you used our services, we promised to keep your personal health information private. The United States Department of Justice ("DOJ") and the Federal Trade Commission ("FTC") allege that we shared health information about you with other companies without your approval. We have entered into an agreement with the DOJ and the FTC relating to the sharing of this information.

What happened?

The DOJ and the FTC allege that we shared information about you, including the fact that you signed up or paid for our alcohol addiction treatment services, and information that companies could use to identify you, with AdRoll, Amazon, Google, Impact, LiveIntent, Meta (formerly Facebook), Microsoft, Pinterest, PowerInbox, Quora, and Reddit.

The DOJ and the FTC allege that these companies often linked this information to your accounts on their platforms so we could show ads to you or people like you.

What are we doing in response?

To resolve the case:

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

Learn more

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

To learn more about the settlement, go to ftc.gov/Monument.