UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

D.M., individually and on behalf of all others similarly situated, Plaintiff, v. **MONUMENT, INC.,** Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff D.M. brings this class action complaint on behalf of himself, and all others similarly situated (the "Class Members") against Monument, Inc. ("Monument" or "Defendant"). The allegations contained in this class action complaint are based on Plaintiff's personal knowledge of facts pertaining to himself and upon information and belief, including further investigation conducted by Plaintiff's counsel.

NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of a nationwide class to address Defendant's improper, unauthorized, and illegal disclosure of Class Members' personally identifiable information ("PII") and/or protected health information ("PHI") (collectively referred to as "Private Information") through intentional use of Tracking Technologies to third-party advertising platforms such as Meta, Google, Bing, Pinterest and others.

2. Information about a person's mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace or denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone

other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

3. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the United States Department of Health and Human Services ("HHS") has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers and their business associates must safeguard and protect Private Information. Under the HIPAA Privacy Rule, **no** health care provider or business associate can disclose a person's personally identifiable protected health information to a third party without express written authorization. 45 C.F.R. §164.502(a)

4. Defendant has developed, advertised, and offered for sale an online mental health platform for the treatment of alcohol dependency that matches users with affiliated physicians and facilitates counseling via Defendant's websites, including but not limited to www.joinmonument.com. In May 2022 Defendant acquired Tempest, a platform providing similar services as Monument.[1] Defendant's separate websites, including Tempest, are collectively referred to herein as "Defendant's Website" or the "Website."

5. Thousands of users have signed up for Defendant's services. In doing so, those customers entrusted Defendant with their Private Information, including their name, date of birth, email address, telephone number, address, Monument ID, insurance member ID, IP address, unique digital ID, Uniform Resource Locator (URL), photograph, selected services or plan, assessment or survey responses, appointment-related information, and associated health information relating to alcohol dependency treatment.

6. Recognizing the sensitivity of this Private Information, Defendant repeatedly promised to keep it anonymous and private and use it only for lawful purposes such as to facilitate consumers' treatment.

[1] *Big News! Tempest Joins the Monument Family*, Tempest (May 17, 2022), https://jointempest.com/resources/big-news-tempest-joins-the-monument-family.

7. Rather than protecting Plaintiff's and Class Members' confidential and sensitive Private Information, however, Defendant installed Pixels and other code on its Website to track users and collect data and information about them that it could later monetize ("Tracking Technologies").

8. Defendant continually broke its promises to protect consumers' Private Information, instead using it to target existing and new customers with advertising for its services. Defendant also handed over Plaintiff's and Class Members' Private Information to some of the largest online advertising companies in the world, such as Meta, Google, Bing, and Pinterest, often permitting these companies to use the sensitive Private Information for their own research, product development, and advertising purposes.

9. Defendant: (i) failed to employ reasonable measures to safeguard Private Information it collected from users; (ii) failed to properly train its employees to protect Private Information when using it for advertising; (iii) failed to properly supervise staff in the use of Private Information; (iv) failed to provide users with proper notice as to the collection, use, and disclosure of their Private Information; and (v) failed to limit how third parties could use users' Private Information.

10. The Federal Trade Commission ("FTC") Director for the Bureau of Consumer Protection, Samuel Levine, recently stated, "[d]igital health companies and mobile apps should not cash in on consumers' extremely sensitive and personally identifiable health information," noting that the sale of this information constituted blatant "misuse and illegal exploitation."[2]

11. In response to the use of tracking and data collection technologies by companies offering health care services, the Office for Civil Rights at the HHS recently published a bulletin concerning the Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (the "Bulletin").[3] The Bulletin warns that:

[2] *FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising*, Federal Trade Commission (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising.

[3] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dept. of Health and Human Services (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-

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

12. And as recently noted by the Hon. William J. Orrick in a decision concerning the use of the data Tracking Technologies by healthcare organizations, "[o]ur nation recognizes the importance of privacy in general and health information in particular: the safekeeping of this sensitive information is enshrined under state and federal law."[4]

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

JURISDICTION AND VENUE

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

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

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

---

tracking/index.html.

[4] *In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218, at *1 (N.D. Cal. Dec. 22, 2022).

THE PARTIES

17. Plaintiff D.M. is an adult citizen of the State of California, residing in San Diego County. He brings this action anonymously to protect his confidential personal health information, which is protected under HIPAA.

18. Defendant Monument, Inc. is a Delaware corporation with a principal place of business located at 350 7th Avenue, New York, NY, United States, 10001.

19. Defendant does business under various other names in addition to Monument, including Tempest.

FACTUAL ALLEGATIONS

Background

20. Defendant Monument has been in operation since 2018, offering online alcohol dependency treatment and counseling services via various websites and affiliated physicians.

21. Since its inception, Defendant has signed up thousands of users and as of 2022 acquired Tempest, also an online alcohol dependency treatment platform.

22. On or around February 6, 2023, Defendant's internal review concluded that Private Information was shared with Meta, Google, Bing, Pinterest, and other third parties through the use of Tracking Technologies "without the appropriate authorization, consent, or agreements required by law."[5]

23. The Private Information included name, date of birth, email address, telephone number, address, Monument ID, insurance member ID, IP address, unique digital ID, Uniform Resource Locator (URL), photograph, selected services or plan, assessment or survey responses, appointment-related information, and associated health information.[6]

24. According to Defendant, the unauthorized disclosure "commenced in January of 2020, with respect to Monument members, and November of 2017, with respect to Tempest

[5] *Notice*, Office of Attorney General for the State of California (Mar. 28, 2023), https://oag.ca.gov/system/files/Monument%20-%20Sample%20Notification%20Letter%204888-3653-0266%20v.2.pdf.
[6] *Id.*

members."[7]

25. In the ordinary course of receiving services from Defendant, Plaintiff and Class Members were required to provide Defendant with Private Information.

26. Defendant agreed to and undertook legal duties to maintain the Private Information of Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws.

27. As explained below, Defendant's data security policies fail to comply with industry standards.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure.

29. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

30. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosure of this Private Information.

31. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their Private Information which includes information that is static, does not change, and can be used to commit myriad financial crimes.

32. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for authorized business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their Private Information.

33. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties.

[7] *Id.*

34. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the unauthorized disclosure of Private Information.

35. Defendant admitted that Private Information potentially impacted in the unauthorized disclosure contained name, date of birth, email address, telephone number, address, Monument ID, insurance member ID, IP address, unique digital ID, Uniform Resource Locator (URL), photograph, selected services or plan, assessment or survey responses, appointment-related information, and associated health information.

36. Because Defendant failed to properly protect and safeguard Plaintiff's and Class Members' Private Information, unauthorized third parties were able to access Plaintiff's and Class Members' Private information, without prior authorization.

Defendant's Deceptive and Unfair Marketing Practices

37. Defendant has spent significant efforts since inception advertising and marketing its services through various digital and traditional media platforms, including search engine ads, and through third parties such as Meta, Google, Bing, and Pinterest.

38. Defendant markets all of its services by offering online communications with a "24/7 anonymous forum."[8] Monument also claims that its community is "entirely anonymous"[9] and "Monument's platform is 100% secure and confidential."[10]

39. Customers signing up for Defendant's services pay between $9.99 and $249 per month. To sign up for counseling services, a customer must fill out an online intake questionnaire and answer a detailed series of questions about the customer's personal life and mental health, including age, gender, marital/relationship status, whether the customer has ever been in therapy before. The online questionnaire also asks other questions that elicit Plaintiff's and Class Members' Private Information.

[8] *Home*, Monument, https://joinmonument.com (last visited Apr. 15, 2023).
[9] *Community*, Monument, https://joinmonument.com/community (last visited Apr. 15, 2023).
[10] *Therapy Approach*, Monument, https://joinmonument.com/therapy-approach (last visited Apr. 15, 2023).

40. Thousands of Website visitors, including those like Plaintiff and Class Members who ultimately signed up for Defendant's services, were presented with these repeated promises about the confidentiality of the Private Information they shared with Defendant. Despite these promises, however, Defendant used Private Information extensively for Defendant's own profit, including by sharing and disclosing Private Information.

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

41. In exchange for disclosing the Private Information of its patients, Defendant was able to obtain tens or hundreds of thousands of new customers, each of whom paid between $9.99 and $249 per month for Defendant's services.

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

43. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[11]

44. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[12]

IP Addresses Are Personally Identifiable Information

45. Defendant also disclosed Plaintiff's and Class Members' Computer IP addresses.

[11] Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, Time (Jan. 9, 2017), https://time.com/4588104/medical-data-industry/.
[12] Christina Farr, *Hospital execs say they are getting flooded with requests for your health data*, CNBC (Dec. 18, 2019), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

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

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

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

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

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

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

Defendant Failed to Comply with its Own Notice of Privacy Practices

51. Defendant's Notice of Privacy Practices is stated on the Website. It states, "we protect the privacy and security of your substance use disorder patient records in accordance with 42 U.S.C. § 290dd–2 and 42 C.F.R. Part 2, the Confidentiality of Substance Use Disorder Patient Records ("Part 2"), in addition to HIPAA and applicable state law."[13]

52. Defendant also states, "we have elected to voluntarily and substantially comply with the standards set forth in HIPAA."[14]

53. With regards to marketing, Defendant states "[w]e will not use or disclose your health information for marketing purposes without your written authorization except as otherwise

[13] Notice of *Privacy Practices*, Monument (Oct. 5, 2021), https://joinmonument.com/notice-of-privacy-practices/.
[14] *Id.*

permitted by law."[15]

54. In providing alcohol dependency treatment, Defendant stored Plaintiff's and Class Members' Private Information.

55. By disclosing Plaintiff's and Class Members' Private Information through intentional use of Tracking Technologies to third-party advertising platforms such as Meta, Google, Bing, Pinterest and others, Defendant violated its own Notice of Privacy Practices.

56. None of the exceptions that justify permitting disclosure of Plaintiff's and Class Members' Private Information apply to the Defendant's intentional disclosure of Plaintiff's and Class Members' Private Information to third-party advertising platforms such as Meta, Google, Bing, Pinterest and others.

57. Defendant unlawfully disclosed Private Information to third-party advertising platforms, meaning Plaintiff's and Class Members' Private Information was accessed and exfiltrated by unauthorized third parties.

Defendant had an Obligation to Protect Private Information under Federal and State Law and the Applicable Standard of Care

58. Defendant is a Business Associate covered by HIPAA (45 C.F.R. § 160.102). As such, it is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

59. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

60. HIPAA's Security Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is health or transferred in electronic form.

61. HIPAA requires Defendant to "comply with the applicable standards,

[15] *Id.*

implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

62. "Electronic protected health information" is "individually identifiable health information . . . that is (i) Transmitted by electronic media; (ii) maintained in electronic media." 45 C.F.R. § 160.103.

63. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

64. HIPAA also required Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

65. HIPAA also required Defendant to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

66. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the unauthorized disclosure to each affected individual without unreasonable delay and in no case later than 60 days following discovery of the unauthorized disclosure.

67. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce."

The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.* (3d Cir. 2015) 799 F.3d 236.

68. As described before, Defendant is also required (by the CCRA, CMIA, CCPA and various other states' laws and regulations) to protect Plaintiff's and Class members' Private Information, and further, to handle any unauthorized disclosure of the same in accordance with applicable breach notification statutes.

69. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members whose Private Information was entrusted to it to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being disclosed to unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that the Website, and the personnel responsible for maintaining and monitoring it, adequately prevented Plaintiff's and Class Members' Private Information from being disclosed to third parties without Plaintiff's and Class Members' consent.

70. Defendant owed a duty to Plaintiff and Class Members whose Private Information was entrusted to Defendant to design, maintain, and monitor and test the Website to ensure that the Private Information input therein was adequately secured and protected from unauthorized disclosure.

71. Defendant owed a duty to Plaintiff and Class Members whose Private Information was entrusted to Defendant to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who updated and/or monitored the Website on how to adequately protect the Private Information input therein from unauthorized disclosure.

72. Defendant owed a duty to Plaintiff and Class Members whose Private Information was entrusted to Defendant to implement processes that would detect unauthorized disclosures via the Website in a timely manner.

73. Defendant owed a duty to Plaintiff and Class Members whose Private Information was entrusted to Defendant to act upon data security warnings and alerts in a timely fashion.

74. Defendant owed a duty to Plaintiff and Class Members whose Private Information was entrusted to Defendant to adequately train and supervise its employees to identify and avoid any unauthorized disclosure.

75. Defendant owed a duty to Plaintiff and Class Members whose Private Information was entrusted to Defendant to disclose if the Website was inadequate to keep individuals' Private Information protected from unauthorized disclosure because such an inadequacy would be a material fact in the decision to entrust Private Information with Defendant through utilization of the Website.

76. Defendant owed a duty to Plaintiff and Class Members whose Private Information was entrusted to Defendants to disclose in a timely and accurate manner when unauthorized disclosure occurred.

77. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

Defendant Violated Industry Standards

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

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

80. AMA Code of Ethics Opinion 3.1.1 provides:

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

81. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent

> undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de- identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

82. AMA Code of Medical Ethics Opinion 3.3.2 provides:

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

Plaintiff's Experience with Defendant's Website

83. Beginning in December 2022, Plaintiff D.M. sought services from Defendant.

84. Prior to deciding to transact with Defendant, Plaintiff viewed and relied upon Defendant's representations concerning its commitment to maintaining the confidentiality of Private Information communicated by consumers via Defendant's Website. Had Plaintiff known that Defendant would not maintain his Private Information as private and confidential, Plaintiff would not have signed up Defendant's services.

85. Plaintiff reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be disclosed to a third party.

86. On information and belief and based on Defendant's standard practices as described herein, Defendant disclosed Plaintiff's Private Information and communications to third parties, including when he completed questionnaires on Defendant's Website.

87. Through the process detailed in this Complaint, Defendant disclosed Plaintiff's Private Information, including his personally identifiable information, protected health information, and related confidential information, to third parties. Defendant never disclosed to Plaintiff that it would disclose, sell, or otherwise share his Private Information with third parties. Instead, Defendant disclosed Plaintiff's Private Information without Plaintiff's knowledge,

consent, or express written authorization.

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

CLASS ACTION ALLEGATIONS

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

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

> All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through a Monument Website (including but not limited to joinmonument.com and jointemptest.com).

91. The California Class that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the State of California whose Private Information was disclosed to a third party without authorization or consent through a Monument Website (including but not limited to joinmonument.com and jointemptest.com).

92. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including its staff and immediate family.

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

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

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

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant violated its Notice Privacy Practices by disclosing the PII and PHI of Plaintiff and Class Members to Meta, Google, Bing, Pinterest, and/or additional third parties;

d. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been disclosed to third parties without their consent;

f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient PHI and PII;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

h. Whether Defendant violated the consumer protection statutes invoked herein;

i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Defendant knowingly made false representations as to its data security and/or Notice of Privacy Practices; and

k. Whether Defendant knowingly omitted material representations with respect to its data security and/or Notice of Privacy Practices.

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

97. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent

and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

98. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

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

100. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the

limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

101. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

103. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members from unauthorized disclosure to third parties via the Tracking Technologies implemented on the Website. Defendant may also continue to refuse to provide proper notification to Class Members regarding the practices complained of herein and may thus continue to act unlawfully as set forth in this Complaint.

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

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

a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;

b. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members'

Private Information with respect to Defendant's Notice of Privacy Practices;

c. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties; and

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

106. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

107. Plaintiff and the Class entrusted Defendant with their Private Information.

108. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for authorized business purposes only, and not disclose their Private Information to unauthorized third parties.

109. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

110. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class

involved an unreasonable risk of harm to Plaintiff and the Class.

111. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant assumed a duty to protect Plaintiff's and Class Members' Private Information.

112. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant assumed and/or had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class Members in Defendant's possession through use of Defendant's Website was adequately secured and protected.

113. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information through their use of the Website, Defendant assumed and/or had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain pursuant to regulations.

114. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information through their use of the Website, Defendant assumed and/or had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

115. By installing some safeguards to protect Plaintiff's and Class Members' Private Information, Defendant assumed and/or had a duty to properly safeguard Plaintiff's and Class Members' Private Information.

116. The harm that occurred as a result of the unauthorized disclosure is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

117. Defendant's duty to use reasonable security measures on the Website arose as a

result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

118. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

119. Unauthorized access and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

120. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information collected through and/or stored on Defendant's Website.

121. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the unauthorized disclosure as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

122. Defendant knew or should have known that Plaintiff's and Class Members' Private Information was stored on its network and was or should have been aware of the extreme risks associated with failing to properly safeguard Plaintiff's and Class Members' Private Information.

123. Defendant was or should have been aware that the likelihood of an unauthorized disclosure was foreseeable, based on published guidance on the usage of Tracking Technologies by organization collecting and storing Private Information.

124. Despite knowing Tracking Technologies were being used on its Website, Defendant failed to correct, update, or upgrade its data security protections, thus causing the unauthorized disclosure.

125. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

126. Defendant was in the best position to protect against the harm suffered by Plaintiff and the Class as a result of the unauthorized disclosure.

127. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession was disclosed to unauthorized third parties, how it was disclosed, and precisely the types of data that were disclosed, to whom these types of data were disclosed, and when such disclosure took place, and then to repair any harm or imminent future risk of harm that Plaintiff and Class Members have suffered as a result.

128. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

129. Defendant has admitted that the Private Information of Plaintiff and Class Members was disclosed due to Defendant's use of Tracking Technologies and thus also accessed and exfiltrated by unauthorized third persons as a result of the unauthorized disclosure.

130. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendant's possession or control.

131. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the unauthorized disclosure.

132. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiff and the Class in the face of increased risk of unauthorized disclosure through the use of Tracking Technologies.

133. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

134. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Private Information it was no longer required to retain pursuant to regulations.

135. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the unauthorized disclosure.

136. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Private Information of Plaintiff and the Class would not have been compromised.

137. Said differently, if Defendant had properly prevented the use of Tracking Technologies disclosing Plaintiff's and Class Member's Private Information, then the unauthorized disclosure would not have occurred, and Plaintiff's and Class Members' Private Information would have been appropriately safeguarded.

138. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

139. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate data security practices to safeguard Plaintiff's and Class Members' Private Information.

140. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

141. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described

in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

142. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

143. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

144. The harm that occurred as a result of the unauthorized disclosure is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

145. Moreover, pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

146. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.

147. Defendant breached its duties to Plaintiff and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiff's and Class Members' Private Information.

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

149. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

150. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that

it was failing to meet its duties, and that the unauthorized sharing of Plaintiff's and Class Members' highly sensitive Private Information with unauthorized third parties via the use of Tracking Technologies on the Website would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

151. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the unauthorized disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the unauthorized disclosure for the remainder of the lives of Plaintiff and the Class.

152. As a direct and proximate result of Defendant' negligence and negligence per se, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

153. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to

further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

154. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

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

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

157. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

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

159. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information to third parties, including Meta, Google, Bing, Pinterest, and others.

160. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein. Plaintiff and Class Members would not have used Defendant's services, or would have paid substantially less for these services, had they known their Private Information would be disclosed.

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

COUNT II
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200
(On behalf of Plaintiff and the California Class)

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

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

164. Defendant engaged in unlawful business practices in connection with its disclosure of Plaintiff's and Class Members' Private Information to unrelated third parties, including Meta, Google, Bing, Pinterest, and others, in violation of the UCL.

165. The acts, omissions, and conduct of Defendant took place in California. Defendant was doing business in California and advertised to consumers in California.

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

167. Defendant violated the "unlawful" prong of the UCL by violating, inter alia, Plaintiff's and Class Member's constitutional rights to privacy, state and federal privacy statutes, and state consumer protection statutes, such as HIPAA and the California Confidentiality of Information Act ("CMIA"). Defendant also violated the unlawful prong of the UCL by disseminating false and misleading statements regarding its privacy practices in violation of California's False Advertising Laws.

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

169. Defendant's acts, omissions, and conduct also violate the fraudulent prong of the

UCL because Defendant made material misrepresentations and omissions of fact to induce Plaintiff and Class Members to purchase Defendant's services without disclosing that Defendant shared, used, and sold Plaintiff's and Class Members Private Information and without obtaining consent. Defendant represented that it would keep Plaintiff's and Class Members' Private Information anonymous, when in fact it did not. Defendant's acts, omissions, nondisclosures, and misleading statements as alleged herein were and are false, misleading, and/or likely to deceive the consuming public.

170. Plaintiff viewed and relied upon Defendant's representations concerning the anonymity and confidentiality of information provided by Plaintiff and Class Members to Defendant. Had Defendant disclosed that it shared Private Information with third parties, Plaintiff would not have signed up Defendant's services.

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

172. As result of Defendant's violations of the UCL, Plaintiff and Class Members have suffered injury in fact and lost money or property, including but not limited to payments to Defendant and/or other valuable consideration, *e.g.*, access to their private and personal data. The unauthorized access to Plaintiff's and Class Members' private and personal data also has diminished the value of that information.

COUNT III
VIOLATION OF CALIFORNIA FALSE ADVERTISING LAW
Cal. Bus. & Prof. Code § 17500
(On behalf of Plaintiff and the California Class)

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

174. The acts, omissions, and conduct of Defendant took place in California. Defendant was doing business in California and advertised to consumers in California.

175. California's False Advertising Law, Cal. Bus. & Prof. Code § 17500, et seq., makes

it "unlawful for any person to make or disseminate or cause to be made or disseminated before the public in this state, … in any advertising device … or in any other manner or means whatever, including over the Internet, any statement, concerning … personal property or services, professional or otherwise, or performance or disposition thereof, which is untrue or misleading and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading.

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

177. Defendant's statements include but are not limited to representations and omissions made to consumers on the Website and Notice of Privacy Practices regarding Defendant's commitment to maintain the confidentiality and privacy of Private Information and not to disclose Private Information to third parties. Such representations and omissions constitute false and deceptive advertisements.

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

179. Defendant's actions in violation of § 17500, as described herein, were false and misleading such that the general public is and was likely to be deceived. Plaintiff and the members of the Class were deceived by Defendant's statements and omissions made online when they signed up and started paying for Monument services, and there is a strong probability that consumers and members of the public were also or are likely to be deceived as well. Any reasonable consumer

would be misled by Defendant's false and misleading statements and material omissions. Plaintiff and other members of the Class did not learn of Defendant's disclosure of their Private Information until after they had already signed up and paid for Defendant's service. They relied on Defendant's statements and omissions to their detriment.

180. Plaintiff and the Class lost money or property as a result of Defendant's violations of the False Advertising Law because they would not have signed up for Defendant's services on the same terms if the true facts were known about the product and Defendant's services do not have the characteristics as promised by Defendant. Plaintiff, individually and on behalf of all similarly situated consumers, seeks individual, representative, and public injunctive relief and any other necessary orders or judgments that will prevent Defendant from continuing with its false and deceptive advertisements and omissions; restitution that will restore the full amount of their money or property; disgorgement of Defendant's relevant profits and proceeds; and an award of costs and reasonable attorneys' fees.

COUNT IV
VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT
Cal. Civ. Code § 56, *et seq.*
(On behalf of Plaintiff and the California Class)

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

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

183. Defendant is a healthcare provider as defined by Cal. Civ. Code § 56.06.

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

185. As set forth above, name, date of birth, email address, telephone numbers, address, Monument ID, insurance member ID, IP address, unique digital ID, Uniform Resource Locator (URL), photograph, selected services or plan, assessment or survey responses, appointment-related information, and associated health information relating to alcohol dependency treatment, and other characteristics that can uniquely identify Plaintiff and Class members are transmitted to in combination with patient health concerns, treatment(s) sought, medications, and whether the patient is suffering from alcohol use disorder, or a number of other health symptoms. This protected health information and personally identifiable information constitutes confidential information under the CMIA. This information is collected, recorded, and stored by Defendant and intentionally disclosed to third parties without Plaintiff's and Class Members' knowledge or consent.

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

187. As set forth above, Meta, Google, Bing and Pinterest, and other third parties view, process, and analyze the confidential medical information they receive from Defendant and use that Private Information for advertising and marketing purposes.

188. As demonstrated herein above, Defendant failed to obtain its patients' authorization for the disclosure of medical information and fails to disclose on its Notice of Privacy Practices that it shares protected health information with third parties for marketing purposes.

189. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical information must be: (1) "Clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization;" (2)

signed and dated by the patient or her representative; (3) state the name and function of the third party that receives the information; (4) state a specific date after which the authorization expires. Accordingly, the information set forth in Defendant's Notice of Privacy Practices and any Terms and Conditions do not qualify as a valid authorization.

190. Based on the above, Defendant is violating the CMIA by disclosing its patients' medical information to third parties along with the patients' individually identifying information. Accordingly, Plaintiff and Class Members seek all relief available for Defendant's CMIA violations.

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

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class)

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

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

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

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

196. The benefits that Defendant derived from Plaintiff and Class Members were not offered by Plaintiff and Class Members gratuitously and rightly belong to Plaintiff and Class

Members. It would be inequitable under unjust enrichment principles for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

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

RELIEF REQUESTED

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

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

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

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

DEMAND FOR JURY TRIAL

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

DATED: May 30, 2023

Respectfully Submitted,

By: */s/ Mason A. Barney*

Mason A. Barney
SIRI & GLIMSTAD, LLP
745 Fifth Ave, Suite 500
New York, NY 10151
Telephone: 212-532-1091
mbarney@sirillp.com

Marcus J. Bradley*
Kiley L. Grombacher*
Fernando Valle, Jr.*
BRADLEY/GROMBACHER LLP
31365 Oak Crest Dr., Suite 240
Westlake Village, CA 91361
Telephone: 805-270-7100
mbradley@bradleygrombacher.com
kgrombacher@bradleygrombacher.com
fvalle@bradleygrombacher.com

**pro hac vice forthcoming*

Attorneys for Plaintiff and the Putative Class

ClassAction.org
