John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Fax: (865) 522-0049
Email: jnelson@milberg.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

BARAK FEDERMAN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CEREBRAL INC., a Delaware corporation,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Barak Federman ("Plaintiff") brings this Class Complaint against Cerebral Inc. (“Cerebral” or “Defendant”) and alleges, upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows:

JURISDICTION

1. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs; and minimal diversity exists because at least one class member, including Plaintiff, and Defendant are citizens of different states.

2. This Court has federal question jurisdiction under 29 U.S.C. § 1331 because this Complaint alleges violations of the ECPA (28 U.S.C. § 2511, *et seq*., and 28 U.S.C. § 2702) and the CFAA (18 U.S.C. § 1030, *et seq*).

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

PARTIES

Plaintiff Barak Federman

4. Plaintiff Barak Federman is a citizen and resident of New York.

5. Plaintiff Federman has received healthcare services from Defendant since 2022 and accessed those services via Defendant’s website and mobile

applications ("Digital Platforms"). While using Defendant's Digital Platforms, Plaintiff communicated sensitive, and what he presumed to be confidential, personal and medical information to Defendant.

6. Plaintiff Federman used Defendant's Digital Platforms to communicate with healthcare providers, research particular medical concerns and treatments, fill out forms and questionnaires, schedule and attend appointments, and perform other tasks related to his specific medical inquiries.

7. In the course of using Defendant's services, Plaintiff provided his name, phone number, email address, date of birth, and other PII. As a result of the Tracking Pixel Defendant chose to install on its Digital Platforms, this information was intercepted, viewed analyzed, and used by unauthorized third parties.

8. In the course of using Defendant's services, Plaintiff answered Cerebral's online mental health self-assessment and communicated information regarding his particular health condition and concerns and other PHI. As a result of the Tracking Pixel Defendant chose to install on its Digital Platforms, this information was intercepted, viewed analyzed, and used by unauthorized third parties.

9. In the course of using Defendant's services, Plaintiff communicated to and received from Defendant information regarding his appointments, treatments, clinical information, health insurance and pharmacy information, and insurance information. As a result of the Tracking Pixel Defendant chose to install on its Digital

Platforms, this information was intercepted, viewed analyzed, and used by unauthorized third parties.

10. Plaintiff Federman has been a Cerebral user since 2022.

11. Plaintiff Federman accessed Defendant's Digital Platforms to receive healthcare services from Defendant or Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

12. As Defendant's patient, Plaintiff Federman reasonably expected that his online communications with Defendant were solely between himself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Federman also relied on Defendant's Privacy Policies in reasonably expecting Defendant would safeguard his Private Information. But for his status as Defendant's patient and Defendant's representations via its Privacy Policies, Plaintiff Federman would not have disclosed his Private Information to Defendant.

13. During his time as Defendant's patient, Plaintiff Federman never consented to the use of his Private Information by third parties or to Defendant enabling third parties, including Facebook, Google, TikToK, and others to access or interpret such information.

14. Notwithstanding, through the Tracking Pixel and similar technologies embedded on Defendant's Digital Platforms, Defendant transmitted Plaintiff Federman's Private Information to third parties, including Facebook, Google, TikTok, and others.

15. Facebook, Google, TikTok, and others offer code to website and mobile application operators, like Defendant, to integrate into their platforms. When a user accesses a platform hosting the Pixel, the Pixel's software script surreptitiously directs the user's browser to send a separate message to a third party's servers during their interaction with the webpage. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Pixel is configured to collect. This transmission is initiated by the code concurrently with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's Websites—Defendant's own code, and the Pixel embedded code.

16. After intercepting and collecting this information, Facebook, Google, TikTok, and others view it, process it, analyze it, and assimilate it into data sets used to target consumers with advertising.

17. The Private Information of Plaintiff's and Class Members' that was unlawfully intercepted and transmitted by Defendant includes: names, phone numbers, email addresses, dates of birth, IP addresses, Cerebral client ID numbers, and other demographic or information.

18. According to the report Defendant submitted to the United States Department of Health and Human Services, Defendant admits that the Private Information of at least 3,000,000 individuals was improperly and unlawfully

disclosed to Facebook, Google, TikTok, and others without those individuals' knowledge or consent.

19. Plaintiff brings this complaint to address Defendant's transmission and disclosure of Plaintiff's and Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information" or "PII and PHI") to Meta Platforms, Inc. d/b/a Meta ("Facebook") and/or Google LLC d/b/a Google ("Google") via a tracking pixel ("Tracking Pixel" or "Pixel") installed on Defendant's website.

Defendant Cerebral Inc.

20. Defendant Cerebral Inc. is a healthcare company incorporated in Delaware with its with its principal place of business and headquarters located at 340 S. Lemon Ave., #9892, Walnut, California, 91789.

VENUE

21. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District and a substantial part of the acts and omissions complained of herein took place in this District.

NATURE OF THE ACTION

22. Defendant is a healthcare corporation headquartered in California. Defendant " offers long-term online care and medication management for a wide range of mental health conditions."[1]

23. Plaintiff brings this case to address Defendant's transmission and disclosure of Plaintiff's and Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information") to Meta Platforms, Inc. d/b/a Meta ("Facebook") and/or Google LLC d/b/a Google ("Google") via a tracking pixel ("Tracking Pixel" or "Pixel") installed on Defendant's website.

24. Defendant unlawfully intercepted and transmitted Plaintiff's and Class Members' Private Information including their: names, phone numbers, email addresses, dates of birth, IP addresses, Cerebral client ID numbers, and demographic and other information.

25. In order to provide medical treatment and care, Defendant collects and stores its patients' Private Information and medical records. In doing so, Defendant has statutory, regulatory, contractual, fiduciary, and common law duties to safeguard that Private Information from disclosure and ensure that it remains private and confidential. Defendant is duty bound to maintain the confidentiality of patient

[1] https://cerebral.com/faqs#General_questions-How_does_Cerebral_work_ (last visited Mar. 9, 2023).

medical records and information and is further required to do so by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[2]

26. According to a report Defendant submitted to the United States Department of Health and Human Services, Defendant admits that the Private Information of at least 3,000,000 individuals was improperly and unlawfully disclosed to Facebook and Google without those individuals' knowledge or consent.[3]

27. Plaintiff and Class Members are individuals who are seeking or have sought medical services and/or treatment from Defendant. Defendant advertises its online services on its Digital Platforms and elsewhere to assist patients with their medical care. Based on Defendant's solicitations that patients use its online services, Plaintiff used Defendant's Website to communicate with healthcare providers, research particular medical concerns and treatments, fill out forms and questionnaires, schedule and attend appointments, and perform other tasks related to his particular medical concerns.

[2] The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996), ("HIPAA"), and regulations of the United States Department of Health and Services ("HHS") promulgated thereunder, are designed to protect the confidentiality and guard against the unauthorized disclosure of medical records, patient health care information, and other individually identifiable healthcare information.

[3] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Mar. 9, 2023).

28. Defendant's Privacy Policies ("Privacy Policies") unequivocally state that Defendant will not share Plaintiff's and Class Members' Private Information for marketing purposes unless patients provide written permission.[4]

29. As explained below, however, Defendant did disclose Plaintiff's and Class Members' Private Information via the Tracking Pixel and other technologies to third parties, such as Facebook, Google, TikTok, and others. Defendant's disclosure of Plaintiff's and Class Members' Private Information constitutes a gross violation of common law and statutory data privacy laws.

30. Despite warnings that healthcare organizations were disclosing Private Information to digital marketing companies by incorporating the Tracking Pixel and similar technologies as far back as June of 2022,[5] Defendant did not acknowledge the Tracking Pixel and its widespread and blatant disclosures of Plaintiff's and Class Members' Private Information until on or around March 6, 2023.[6]

31. On or about March 6, 2023, Defendant posted a Statement (hereinafter referred to as the "Notice Letter") on its website, which states the following:

> Cerebral Inc. ("Cerebral") takes your privacy seriously. We write to provide transparency regarding Cerebral's prior data sharing practices via Tracking Technologies (as defined below) on portions of its websites and mobile applications ("Cerebral's Platforms") and with certain subcontractors and other service providers ("Subcontractors").

[4] https://cerebral.com/privacy-policy (last visited Mar. 9, 2023).

[5] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

[6] : https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf

What Happened?

Like others in many industries, including health systems, traditional brick and mortar providers, and other telehealth companies, Cerebral has used what are called "pixels" and similar common technologies ("Tracking Technologies"), such as those made available by Google, Meta (Facebook), TikTok, and other third parties ("Third Party Platforms"), on Cerebral's Platforms. Cerebral has used Tracking Technologies since we began operations on October 12, 2019. Cerebral recently initiated a review of its use of Tracking Technologies and data sharing practices involving Subcontractors. On January 3, 2023, Cerebral determined that it had disclosed certain information that may be regulated as protected health information ("PHI") under HIPAA to certain Third Party Platforms and some Subcontractors without having obtained HIPAA-required assurances.

What Information Was Involved?

The information disclosed varied depending on what actions you took on Cerebral's Platforms, the nature of the services provided by the Subcontractors, the configuration of Tracking Technologies when you used our services, the data capture configurations of the Third-Party Platforms, how you configured your device and browser, and other factors.

- If you created a Cerebral account, the information disclosed may have included your name, phone number, email address, date of birth, IP address, Cerebral client ID number, and other demographic or information.

- If, in addition to creating a Cerebral account, you also completed any portion of Cerebral's online mental health self-assessment, the information disclosed may also have included your selected service, assessment responses, and certain associated health information.

- If, in addition to creating a Cerebral account and completing Cerebral's online mental health self-assessment, you also purchased a subscription plan from Cerebral, the information disclosed may also have included subscription plan type, appointment dates and other booking information, treatment, and other clinical information, health

> insurance/ pharmacy benefit information (for example, plan name and group/ member numbers), and insurance co-pay amount.[7]

32. Parsing out Defendant's Notice Letter, Defendant has admitted that its Website contain a Tracking Pixel that secretly enabled the unauthorized transmission and disclosure of Plaintiff's and Class Members' Private Information to third parties such as Facebook, Google, TikTok and others.

33. The Private Information that Defendant discloses through the Tracking Pixel and similar technologies is valuable to internet marketing companies like Facebook, Google, TikTok, and others as they receive, view, analyze, and aggregate the information to build consumer profiles to assist advertisers in targeting desired demographics.

34. Accordingly, the purpose of this lawsuit is to protect Plaintiff's and Class Members' right to protect their Private Information, to choose who receives it and how it is used, and to seek remedies for the harm caused by Defendant's intentional, reckless, or negligent disclosure to unauthorized third parties.

FACTUAL ALLEGATIONS

Background.

35. A pixel is a piece of code that "tracks the people and [the] type of actions they take."[8] Pixels are routinely used to target specific customers by utilizing the data

---

[7] *Id.*

[8] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Nov. 14, 2022).

gathered through Defendant's pixel to build profiles for the purposes of retargeting and future marketing.[9] The Tracking Pixel is embedded on Defendant's Digital Platforms such that when a visitor interacts with the Digital Application two signals are sent in tandem, one to the intended recipient, Defendant, and another to the unauthorized recipient.

36. Accordingly, when an individual visits Defendant's Digital Platforms and communicates Private Information to Defendant, the Tracking Pixel allows unauthorized to listen in to Plaintiff's and Class Member's communications with Defendant in real time, i.e., they receive the communication as it is communicated to Defendant.

37. Defendant acknowledges that the aggregate information captured by the Tracking Pixel and disclosed to unauthorized parties includes both identifying information, like names and dates of birth, and medical information. The recipients of this data are able to associate information communicated across multiple visits to the Digital Platforms by capturing persistent identifiers like IP addresses, browser fingerprints, and device IDs.

38. Facebook Google, TikTok and others also use cookies installed on Plaintiff's and Class Members' browser to associate Private Information with

[9] "Retargeting" or "remarketing" is a form of advertising that displays ads or sends emails to previous visitors of a particular website who did not "covert" the visit into a sale or otherwise meet a marketing goal of the website owner.

particular individuals. For example, with respect to Facebook, the persistent Tracking Pixel on Defendant's Website causes that individual's unique and persistent Facebook ID ("FID") to be transmitted alongside other Private Information that is sent to Facebook.

39. Upon information and belief, Defendant utilized the Pixel data to improve and save costs on its marketing campaign, improve its data analytics, attract new patients, and market new services and/or treatments to its existing patients. In other words, Defendant implemented the Tracking Pixel to bolster its profits.

40. Pixels are routinely used to target advertising to specific consumers by utilizing the data gathered through the pixel to build profiles for the purposes of retargeting and future marketing.

41. In this context, the Tracking Pixel is designed to transmit to third parties data gathered about the web page currently visited and any information to/from the User to the web page. In other words, a pixel creates a link – hidden from the Digital Platform's user – that transfers information sent to/from the web page to the third party.

42. Operating as designed, Defendant's Tracking Pixel allowed the Private Information that Plaintiff and Class Members communicated to Defendant to be unlawfully disclosed to third parties.

43. For example, when Plaintiff or a Class Member accessed Defendant's Website hosting the Pixel, the Pixel software directed Plaintiff's or Class Members'

browser to send a message to the third party's servers alongside the message intended for Defendant's server. The information sent to third parties by Defendant included the Private Information that Plaintiff and Class Members submitted to Defendant's Digital Platform. Such Private Information would allow the third party (*e.g.,* Facebook or Google) to know that a specific patient was seeking confidential medical care and the type of medical care being sought.

44. The third party, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers who online target[10] Plaintiff and Class Members based on communications obtained via the Tracking Pixel.

45. Plaintiff submitted personal and medical information to Defendant's Digital Platforms and used the Digital Platforms to communicate with healthcare providers, research particular medical concerns and treatments, fill out forms and questionnaires, schedule and attend appointments, and perform other tasks related to his particular medical concerns.

46. Via the Tracking Pixel, Defendant transmitted this Private Information to third parties, such as Facebook and Google.

[10] "Online Targeting" is "a process that refers to creating advertisement elements that specifically reach out to prospects and customers interested in offerings. A target audience has certain traits, demographics, and other characteristics, based on products or services the advertiser is promoting." See https://digitalmarketinggroup.com/a-guide-to-onlinetargeting-which-works-for-your-business/ (last visited: January 23, 2023).

47. Defendant regularly encouraged Plaintiff and Class Members to use its digital tools, including its Website, to receive healthcare services. In doing so, Defendant also directed Plaintiff and Class Members to its Privacy Policies, which preclude the transmission or disclosure of Private Information to unauthorized third parties, such as Facebook or Google.

48. Plaintiff and Class Members provided Private Information to Defendant in order to receive medical services and with the reasonable expectation that Defendant would protect their Private Information.

49. At all times that Plaintiff and Class Members visited and utilized Defendant's Digital Platforms, they had a reasonable expectation of privacy in the Private Information collected through Defendant's Digital Platforms, including that it would remain secure and protected and only utilized for necessary purposes. Plaintiff's and Class Members' expectations were entirely reasonable because (1) they are patients; and (2) Defendant is a healthcare provider which is required by common and statutory law to protect its patients' Private Information. Moreover, Plaintiff and Class Members also relied on Defendant's Privacy Policies, which do not permit the transmission or disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties.

50. Defendant further made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that they exchange with Defendant. Instead,

Defendant chose to exchange the Private Information to optimize the delivery of its ads, measure cross-device conversions, create custom advertising groups or "audiences," learn about the use of its Digital Platforms, and decrease advertising and marketing costs.[11]

51. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiff's and Class Members' Private Information safe, secure, and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

52. However, as set forth more fully below, Defendant failed in its obligations and promises by utilizing the Tracking Pixel on its Digital Platforms knowing that such technology would transmit and disclose Plaintiff's and Class Members' Private Information to unauthorized third parties.

53. The exposed Private Information of Plaintiff and Class Members can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting or to insurance companies utilizing the information to set insurance rates.

[11] *Id.*

54. While Defendant willfully and intentionally incorporated the Tracking Pixel into its Digital Platforms, Defendant did not disclose to Plaintiff or Class Members that it shared their sensitive and confidential communications via the Tracking Pixel to Facebook or Google until on or around March 6, 2023.

55. As a result, Plaintiff and Class Members were unaware that their Private Information was being surreptitiously transmitted and/or disclosed to Facebook and Google as they communicated with their healthcare provider via the Digital Platforms.

56. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web based technology to ensure Defendant's Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the consent from Plaintiff and Class Members before disclosing their Private Information to Facebook, Google, or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Tracking Pixels; and (v) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

57. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy, (ii) loss of control over their Private Information, (iii) diminution of value of the Private Information, (iv) statutory damages, and (v) the continued and ongoing risk of exposure and use of their Private Information by marketing companies.

Defendant Improperly Disclosed Plaintiff's and Class Members' Private Information via the Tracking Pixel.

58. Defendant incorporated Tracking Pixels and similar technology to better understand the efficacy of its marketing efforts, how users interact with their Digital Platforms and to attract users like Plaintiff and Class Members to Defendant's Digital Platforms with the ultimate goal of increasing profitability. The Pixel and similar technologies were invisible to Plaintiff and Class Members and unbeknownst to them were used to secretly track their interactions by simultaneously transmitting their activity to third party tracking technology providers.

59. While seeking and using Defendant's services as a medical provider, and utilizing the Website, Plaintiff's and Class Members' Private Information was intercepted in real time and then disseminated to Facebook, Google, TikTok, and other third parties, via the Pixel that Defendant secretly installed on its Website.

60. Plaintiff and Class Members did not intend or have any reason to suspect their Private Information would be shared with third parties, or that Defendant was tracking their every communication and disclosing the same to third parties when they entered highly sensitive information on Defendant's Digital Platforms.

61. Defendant did not disclose to or warn Plaintiff or Class Members that Defendant used Plaintiff's and Class Members' confidential electronic medical communications and Private Information for marketing purposes.

62. Defendant tracked Plaintiff's and Class Members' Private Information via the Tracking Pixel.

63. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information.

64. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value as evidenced by its marketing value, has been damaged and diminished by its unauthorized release to Facebook, Google, TikTok, and others, to whom it is now available and holds significant value. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

65. Defendant also deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (i.e., the Tracking Pixel) that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Facebook, Google, and/or other unauthorized third-parties; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

Defendant's Pixel, Source Code, and Interception of HTTP Requests.

66. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as computer, tablet, or smart phone) accessed web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

67. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

68. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can

store and communicate data when visiting one website to an entirely different website.

- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

69. A patient's HTTP Request essentially asks Defendant's Website to retrieve certain information (such as a physician's "Book an Appointment" page), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Webpage(s)).

70. Every webpage is comprised of Markup and "Source Code." Source Code is a set of instructions invisible to the website's visitor that commands the visitor's browser to take certain actions when the webpage first loads or when a specified event triggers the code.

71. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When patients visit Defendant's Digital Platforms via an HTTP Request to Defendant's server, Defendant's server sends an HTTP Response including the Markup that displays the

page of the Digital Platforms visible to the user and Source Code, including Defendant's Pixel. Thus, Defendant is in essence handing patients a tapped phone, and once the Webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook, Google, TikTok, and others.

72. After intercepting and collecting this information, Facebook, Google, TikTok, and others view it, process it, analyze it, and assimilate it into datasets. These datasets allow marketing companies to build intimate profiles concerning an individual's interests, habits, and as here, their concerns or health issues.

73. Third-parties, like Facebook, Google, TikTok, and others, place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the patient associated with the Private Information intercepted.

74. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that cannot be evaded by savvy users. Facebook's workaround, for example, is called Conversions API. Conversions API is an effective workaround because it does not

intercept data communicated from the user's browser. Instead, Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]." Thus, the communications between patients and Defendant, which are necessary to use Defendant's Website, are actually received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

75. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like Conversions API without access to the host server, companies like Facebook instruct Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[12] Thus, it is reasonable to infer that Facebook's customers who implement the Tracking Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround.

76. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user's

[12] *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Jan. 23, 2023).

communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner.

77. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

78. In this case, Defendant employed just such devices (the Tracking Pixel and similar technologies) to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to third parties like Facebook and Google.

Defendant's Privacy Policies and Promises

79. Defendant's Privacy Policies unequivocally state Defendant will not share Plaintiff's and Class Members' Private Information for marketing purposes unless patients provide written permission.[13]

80. Plaintiff and Class Members have not provided Defendant with written permission to share their Private Information for marketing purposes.

81. Despite Defendant's acknowledgement that it will not share Plaintiff's and Class Members' Private Information, Defendant, in fact, shared Plaintiff's and Class Members' Private Information via the Tracking Pixel.

[13] *Id.*

82. Specifically, Defendant transmitted and/or disclosed Plaintiff's and Class Members' Private Information to third parties, like Facebook and Google, without Plaintiff's and Class Members' consent or written permission.

83. In doing so, Defendant intended to improve and save costs on its marketing campaign, improve its data analytics, attract new patients, and market new services and/or treatments to its existing patients.

84. In simple terms, Defendant violated its own Privacy Policy—i.e., the Privacy Policy that Plaintiff and Class Members relied upon—in order to bolster its profits. Defendant Violated HIPAA Standards

Defendant Violated HIPAA Standards.

85. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[14]

86. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

[14] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

87. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[15]

88. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or his protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.* (Emphasis added).[16]

89. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the

[15] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/Deidentification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022)
[16] *Id.*

HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[17]

90. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

91. In other words, HHS has expressly stated that Defendant has violated HIPAA Rules by implementing the Tracking Pixel.

Defendant Violated Industry Standards.

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

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

94. 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)

95. 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

[17] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

> 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. 176. 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 and Class Members' Expectation of Privacy.

96. Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

97. Indeed, at all times when Plaintiff and Class Members provided their PII and PHI to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

IP Addresses are Personally Identifiable Information.

98. On information and belief, through the use of the Tracking Pixels on Defendant's Website, Defendant also disclosed and otherwise assisted Facebook, Google, and/or other third parties with intercepting Plaintiff's and Class Members' Computer IP addresses.

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

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

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

102. Facebook tracks every IP address ever associated with a Facebook user. 184. Google also tracks IP addresses associated with Internet users.

103. Facebook, Google, and other third-party marketing companies track IP addresses for use in tracking and targeting individual homes and their occupants with advertising by using IP addresses.

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

a. 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).

b. 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).

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

Defendant was Enriched and Benefitted from the Use of the Pixel and Unauthorized Disclosures.

106. The sole purpose of the use of the Tracking Pixel on Defendant's Website was to increase marketing efficacy and ultimately profits.

107. In exchange for disclosing the Private Information of its patients, Defendant is compensated by third parties, like Facebook and Google, in the form of the use of the Tracking Pixel and similar technologies.

108. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

109. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients, including Plaintiff and Class Members.

110. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

Defendant Unlawfully Disclosed Plaintiff's Private Information to Facebook and other Third Parties.

Plaintiff Barak Federman

111. Plaintiff Barak Federman entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Federman disclosed his Private Information to Defendant.

112. Plaintiff Federman accessed Defendant's Digital Platforms to receive healthcare services from Defendant and at Defendant's solicitation.

113. Plaintiff Federman used Defendant's Digital Platforms to communicate with healthcare providers, research particular medical concerns and treatments, fill out forms and questionnaires, schedule and attend appointments, and perform other tasks related to his particular medical concerns.

114. In the course of using Defendant's services, Plaintiff provided his name, phone number, email address, date of birth, and other PII. As a result of the Tracking Pixel Defendant chose to install on its Digital Platforms, this information was intercepted, viewed analyzed, and used by unauthorized third parties.

115. In the course of using Defendant's services, Plaintiff answered Defendant's online mental health self-assessment and communicated information regarding his particular health condition and concerns and other PHI. As a result of the Tracking Pixel Defendant chose to install on its Digital Platforms, this information was intercepted, viewed analyzed, and used by unauthorized third parties.

116. In the course of using Defendant's services, Plaintiff communicated to and received from Defendant information regarding his appointments, treatments, clinical information, health insurance and pharmacy information, and insurance information. As a result of the Tracking Pixel Defendant chose to install on its Digital Platforms, this information was intercepted, viewed analyzed, and used by unauthorized third parties.

117. Plaintiff Federman reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

118. Plaintiff Federman provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

119. As described herein, Defendant worked along with Facebook, Google, TikTok, and others to intercept Plaintiff Federman's communications, including those that contained Private Information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

120. Defendant transmitted to third parties Plaintiff Federman's Private Information.

121. On information and belief, as a "redundant" measure to ensure Plaintiff's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's Private Information from electronic storage on Defendant's server directly to Facebook.

122. By doing so without Plaintiff Federman's consent, Defendant breached Plaintiff Federman's right to privacy and unlawfully disclosed Plaintiff Federman's Private Information to third parties.

123. Defendant did not inform Plaintiff Federman that it had shared his Private Information with Facebook until on or around March 6, 2023.

124. Plaintiff Federman suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to his Private Information.

125. Plaintiff Federman has a continuing interest in ensuring that his Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure

TOLLING

126. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that his Private Information was intercepted and unlawfully disclosed because Defendant kept this information secret until Defendant's disclosure on or about March 6, 2023.

CLASS ACTION ALLEGATIONS

127. Plaintiff brings this action on behalf of themselves 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.

128. The Nationwide Class that Plaintiff seek 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 the Tracking Pixel on Defendant's Website.

129. 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 their staff and immediate family.

130. Plaintiff reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate. 297. Numerosity, Fed R. Civ. P. 23(a)(1).

131. The Class Members for each proposed Class are so numerous that joinder of all members is impracticable. Upon information and belief, there are over 3,000,000 million individuals whose Private Information may have been improperly accessed by Facebook and/or Google, and the Class is identifiable within Defendant's records.

132. 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 Privacy Policies by disclosing the PII and PHI of Plaintiff and Class Members to Facebook, Google, 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 compromised;

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 Privacy Policies practices;

k. Whether Defendant knowingly omitted material representations with respect to its data security and/or Privacy Policies practices; and,

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their PII and PHI.

133. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because he had his PII and PHI compromised as a result of Defendant's incorporation of the Pixel and similar technologies, due to Defendant's misfeasance.

134. 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.

135. 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.

136. 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.

137. 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 they 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.

138. 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.

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

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

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

142. 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 Privacy Policies;

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.

143. Plaintiff reserves the right to amend or modify the Class definition as this case progresses

COUNT I
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

144. Plaintiff re-alleges and incorporates by reference all prior paragraphs as if fully set forth herein.

145. Plaintiff's and Class Members' Private Information, including their communications with their healthcare provider and sensitive personal and medical data, are private facts that Defendant disclosed to Facebook, Google, TikTok, and others without the knowledge or consent of Plaintiff and Class Members.

146. Defendant gave publicity to Plaintiff's and Class Members' private facts and the contents of their communications and other data by sharing them with Facebook, Google, TikTok, and others who in turn view and analyze the information and offers it to its advertising partners. Many of those companies have business models predicated on building massive databases of individual consumer profiles from which to sell targeted advertising and make further disseminations.

147. Plaintiff and Class Members had no knowledge that Defendant was tracking and sharing their private browsing activities and communications because Defendant neither disclosed this activity nor acquired Plaintiff's and Class Members' consent to being tracked on Defendant's website or having their activity on the website disclosed to third parties.

148. Defendant's surreptitious tracking and disclosure of Plaintiff's and Class Members' Private Information would be highly offensive to a reasonable person. Particularly given that Plaintiff and Class Members were communicating with their healthcare provider and were not informed that a third party advertiser was listening in on their communications and viewing, acquiring, and using their Private Information.

149. In disseminating Plaintiff's and Class Members' Private Information without their consent in the manner described above, Defendant acted with oppression, fraud, or malice.

150. Plaintiff and Class Members have been damaged by the publication of their Private Information and are entitled to just compensation in the form of actual

damages, general damages, unjust enrichment, nominal damages, and punitive damages.

COUNT II
INVASION OF PRIVACY - INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

151. Plaintiff re-alleges and incorporates by reference all prior paragraphs as if fully set forth herein.

152. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

153. Plaintiff and Class members had a reasonable expectation of privacy in their communications with Defendant via its website and the communications platforms and services therein.

154. Plaintiff and Class members communicated sensitive and protected medical information and individually identifiable information that they intended for only Defendant to receive and that they understood Defendant would keep private.

155. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and

Class members is an intentional intrusion on Plaintiff's and Class members' solitude or seclusion.

156. Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's Privacy Policy and other representations. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will kept confidential. Defendant's disclosure of private medical information coupled with individually identifying information is highly offensive to the reasonable person.

157. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

158. Plaintiff and Class members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

159. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

160. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights.

Such damages are needed to deter Defendant from engaging in such conduct in the future.

161. Plaintiff also seeks such other relief as the Court may deem just and proper.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

162. Plaintiff re-alleges and incorporates by reference all prior paragraphs as if fully set forth herein.

163. 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.

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

165. 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.

166. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information to third parties, i.e., Facebook and/or Google.

167. 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 for these services, had they known their Private Information would be disclosed.

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

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

169. Plaintiff re-alleges and incorporates by reference all prior paragraphs as if fully set forth herein.

170. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

171. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

172. Plaintiff's and Class Members' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its Privacy Policies.

173. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Tracking Pixel to disclose and transmit Plaintiff's Private Information and the contents of their communications exchanged with Defendant to third parties.

174. The third-party recipients included, but were not limited to, Facebook, Google, TikTok and other online marketers.

175. Defendant's disclosures of Plaintiff's and Class Members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

176. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

177. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the provider-patient relationship;

c. Defendant took something of value from Plaintiff and Class members and derived benefit therefrom without Plaintiff's and Class members' knowledge or informed consent and without compensating Plaintiff for the data;

d. Plaintiff and Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

e. Defendant's actions diminished the value of Plaintiff's and Class members' Private Information; and,

f. Defendant's actions violated the property rights Plaintiff and Class members have in their Private Information.

178. Plaintiff and Class Members are therefore entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation.

COUNT V
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(1) *et seq.*
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of Plaintiff and the Class)

179. Plaintiff re-alleges and incorporates by reference all prior paragraphs as if fully set forth herein.

180. The ECPA protects both sending and receipt of communications.

181. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

182. The transmissions of Plaintiff's PII and PHI to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

183. Electronic Communications. The transmission of PII and PHI between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

184. Content. The ECPA defines content, when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

185. Interception. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

186. Electronical, Mechanical, or Other Device. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendant's web-servers; and,

d. The Pixel Code deployed by Defendant to effectuate the sending and acquisition of patient communications

187. By utilizing and embedding the Pixel on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

188. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the Tracking Pixel, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Private Information to third parties such Facebook and Google.

189. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiff's and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

190. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

191. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

192. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

193. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

194. Defendant was not acting under color of law to intercept Plaintiff's and the Class Members' wire or electronic communication.

195. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the Pixel tracking code.

196. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

197. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Website, Defendant's

purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

COUNT VI
VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE 18 U.S.C. § 2511(3)(a)
(On Behalf of Plaintiff and the Class)

198. Plaintiff re-alleges and incorporates by reference all prior paragraphs as if fully set forth herein.

199. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

200. Electronic Communication Service. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

201. Defendant's Website is an electronic communication service. The website provides to users thereof the ability to send or receive electronic communications. In the absence of Defendant's Website, internet users could not send or receive communications regarding Plaintiff's and Class Members' PII and PHI.

202. Intentional Divulgence. Defendant intentionally designed the Tracking Pixel and was or should have been aware that, if misconfigured, it could divulge Plaintiff's and Class Members' PII and PHI.

203. While in Transmission. Upon information and belief, Defendant's divulgence of the contents of Plaintiff's and Class Members' communications was contemporaneous with their exchange with Defendant's Digital Platforms, to which they directed their communications.

204. Defendant divulged the contents of Plaintiff's and Class Members' electronic communications without authorization. Defendant divulged the contents of Plaintiff's and Class Members' communications to Facebook without Plaintiff's and Class Members' consent and/or authorization.

205. Exceptions do not apply. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication as follows:

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"

c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or,

d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency." 18 U.S.C. § 2511(3)(b)

206. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

207. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on Defendant's Website to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant's service; nor (2) necessary to the protection of the rights or property of Defendant.

208. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

209. Defendant's divulgence of the contents of user communications on Defendant's browser through the Pixel code was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As

alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Websites or apps with which Plaintiff and Class Members were exchanging information.

210. Moreover, Defendant divulged the contents of Plaintiff and Class Members' communications through the Tracking Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

211. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

212. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT VII
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (CFAA)
18 U.S.C. § 1030, *et seq.*
(On Behalf of Plaintiff and the Class)

213. Plaintiff re-alleges and incorporates by reference all prior paragraphs as if fully set forth herein.

214. Plaintiff's and the Class's mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

215. Defendant exceeded, and continues to exceed, authorized access to the Plaintiff's and the Class's protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

216. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia,* because of the secret transmission of Plaintiff's and the Class's private and personally identifiable data and content – including the Website visitor's electronic communications with the Website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time ("Website Communications") which were never intended for public consumption.

217. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV) due to the Private Information of Plaintiff and the Class being made available to Defendant, Facebook, and/or other third parties without adequate legal privacy protections.

218. Accordingly, Plaintiff and the Class Members are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."18 U.S.C. § 1030(g).

COUNT VIII
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT
Cal. Pen. Code § 630, *et seq*
(On Behalf of Plaintiff and the Class)

219. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and bring this count individually and on behalf of the proposed Class.

220. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose.

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

221. California Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or **who aids, agrees with, employs, or conspires** with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

222. A defendant must show it had the consent of <u>all</u> parties to a communication.

223. At all relevant times, Defendant aided, employed, agreed with, and conspired with Facebook to track and intercept Plaintiff's and Class Members' internet communications while accessing the Digital Platforms. These communications were transmitted to and intercepted by a third party during the communication and without the knowledge, authorization, or consent of Plaintiff and Class Members.

224. Defendant intentionally inserted an electronic device into its website that, without the knowledge and consent of Plaintiff and Class Members, tracked and transmitted the substance of their confidential communications with Defendant to a third party.

225. Defendant willingly facilitated Facebook's, Google's, TikTok's, and others' interception and collection of Plaintiff's and Class Members' private medical information by embedding the Tracking Pixel on its website.

226. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the Tracking Pixel falls under the broad catch-all category of "any other manner":

- The computer codes and programs Defendant used to track Plaintiff's and Class Members' communications while they were navigating the Digital Platforms;
- Plaintiff's and Class Members' browsers;
- Plaintiff's and Class Members' computing and mobile devices;

- Defendant's web and ad servers;
- The web and ad-servers from which Third Parties tracked and intercepted Plaintiff's and Class Members' communications while they were using a web browser to access or navigate the Digital Platforms;
- The computer codes and programs used by third parties to effectuate their tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit Defendant's Digital Platforms ; and
- The plan Defendant and others carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser or mobile application to visit Defendant's Digital Platforms.

227. Defendant fails to disclose that it is using Tracking Pixel specifically to track and automatically and simultaneously transmit communications to a third party. Defendant is aware that these communications are confidential as its Privacy Policy and representations acknowledge the confidential nature of private medical information and disclaim that it is being shared with unidentified third parties without Plaintiff's and Class Members' express authorization.

228. The patient communication information that Defendant transmits while using Tracking Pixel constitutes protected health information.

229. The Pixel is designed such that it transmits each of the user's actions taken on the webpage to a third party alongside and contemporaneously with the user initiating the communication. Thus, the communication is intercepted in transit to the intended recipient, Defendant and before it reaches Defendant's server.

230. As demonstrated hereinabove, Defendant violates CIPA by aiding and permitting third parties to receive its patients' online communications in real time through its website without their consent.

231. By disclosing Plaintiff's and Class Members' private health information, Defendant violated Plaintiff's and Class Members' statutorily protected right to privacy.

232. As a result of the above violations and pursuant to CIPA Section 637.2, Defendant is liable to the Plaintiff and Class Members for treble actual damages related to their loss of privacy in an amount to be determined at trial or for statutory damages in the amount of $5,000 per violation. Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

233. Under the statute, Defendant is also liable for reasonable attorney's fees, litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

COUNT IX
Violation Of The Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On behalf of Plaintiff and the Class)

234. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

235. Plaintiff brings his claim for injunctive relief as he has no confidence that Defendant has altered its privacy practices and he may wish to use Defendant's services in the future.

236. Plaintiff brings his claim for restitution in the alternative to his claims for damages.

237. 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.

238. Defendant engaged in unlawful business practices in connection with its disclosure of Plaintiff's and Class Members' Private Information to unrelated third parties, including Facebook, in violation of the UCL.

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

240. The acts, omissions, and conduct of Defendant as alleged herein emanated and was directed from Defendant's California headquarters.

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

242. 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, CIPA, the ECPA, and the CFAA as pleaded above.

243. 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 CIPA, the ECPA, and CFAA, and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and Class Members.

244. 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 purchased Defendant's services or would have paid considerably less for those services.

245. The harm caused by the 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.

246. 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.

247. Therefore, Plaintiff and members of the proposed Class are entitled to equitable relief to restore Plaintiff and Class Members to position they would have been in had Defendant not engaged in unfair competition, including an order enjoining Defendant's wrongful conduct, restitution, and disgorgement of all profits paid to Defendant as a result of its unlawful and unfair practices.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Members of the Class defined above, respectfully request that this Court:

A. Certify this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiff as the Class representatives, and appoint the undersigned as Class counsel;

B. Order appropriate relief to Plaintiff and the Class;

C. Enter injunctive and declaratory relief as appropriate under the applicable law;

D. Award Plaintiff and the Class pre-judgment and/or post-judgment interest as prescribed by law;

E. Award reasonable attorneys' fees and costs as permitted by law; and

F. Enter such other and further relief as may be just and proper.

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: March 10, 2023

Respectfully submitted,

s/ *John J. Nelson*
John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Fax: (865) 522-0049
Email: jnelson@milberg.com

Attorneys for Plaintiff and the Putative Class

ClassAction.org
