Samuel M. Ward (SBN 216562)
sward@barrack.com
BARRACK RODOS & BACINE
One America Plaza
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

Counsel for Plaintiffs
[Additional Counsel on Signature Page]

SUPERIOR COURT OF THE STATE OF CALIFORNIA
IN AND FOR THE COUNTY OF LOS ANGELES

STEVEN BELTRAN AND LISA REINGOLD, individually and on behalf of all others similarly situated, Plaintiffs v. CEDARS-SINAI HEALTH SYSTEM AND CEDARS-SINAI MEDICAL CENTER, Defendants	Civil Action No.: 23STCV04041 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Steven Beltran and Lisa Reingold ("Plaintiffs"), individually and on behalf of themselves and all others similarly situated (collectively "Class Members"), by and through their undersigned counsel, brings this class action against Cedars-Sinai Health System and Cedars-Sinai Medical Center (Collectively "Defendants"). Plaintiffs allege as follows upon personal knowledge as to the facts pertaining to themselves individually, and on information and belief as to all other matters.

I. SUMMARY OF THE ACTION

1. Plaintiffs bring this class action versus Defendants for damages arising from Defendants' implementation of software code, embedded in websites and apps maintained and controlled by Defendants, which was created for the purpose of capturing, storing, and sharing the personal data of Plaintiffs and similarly situated consumers. Defendants embedded this software code without the knowledge or authorization of Plaintiffs.

2. Healthcare organizations and providers like Defendants that collect and store patient's private information and medical records have statutory, regulatory, contractual, fiduciary, and common law duties to safeguard that information from disclosure and ensure that it remains private and confidential. Defendants are duty bound to maintain the confidentiality of patient medical patient records and information, and are further required to do so by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and by California law and statute, as more fully discussed below.[1]

3. Indeed, Defendants' knowing implementation of tracking software that collects and discloses patients' private health and identifying information to third parties and marketers, as more fully discussed below, is an egregious breach of the duties imposed on Defendants by law and statute.

4. Plaintiffs bring this class action against Defendants for nominal, compensatory, and punitive damages arising from Defendants' failure to properly secure and safeguard healthcare patients' personally identifiable information and personal health information, such as dates, times, and/or locations

[1] 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 or medical records, patient health care information, medical records, and other individually identifiable healthcare information.

of scheduled appointments; patients' proximity to a Cedars-Sinai location; information about patients' medical providers; and the type of appointment or procedure sought (collectively "Personal Information").

5. Patients of Cedars-Sinai hospital have a reasonable expectation of privacy respecting all forms and content of their communications with Defendants and their affiliated healthcare professionals and systems. They also have a protected interest and right to expect that such information will not be intercepted, transmitted, re-directed, or disclosed to third parties, and that Defendants will not enable their procurement by third parties, including, but not limited to, Facebook, without their prior knowledge, authorization, or consent.

6. Cedars-Sinai patients are encouraged to utilize the Cedars-Sinai mobile app, Cedars Sinai, the patient online portal, My CS-Link, and to use the Cedars-Sinai website, www.cedars-sinai.org, to communicate with Defendants, to make appointments, to find doctors, access medical records, pay and access bills, and to take other actions.

7. To that end, and despite its full knowledge of the private and confidential nature of patients' Personal Information being transmitted, without authorization, to third parties, Defendants configured and implemented a tracking pixel (the "Pixel") to knowingly collect and transmit information from its website to third parties and assist them in procuring confidential healthcare information – including information communicated in sensitive and presumptively confidential patient portals and mobile apps like its CS-Link portal and Cedars-Sinai app.[2] However, unknown to Plaintiffs and users, Defendants did not protect and safeguard patients' Personal Information from access, interception, and procurement by third parties, including Facebook. The Pixel and other tracking software installed on the Cedar-Sinai website was configured so as to enable Defendants and third parties to gather various information collected from visitors to the sites and perform analytics and research on visitors.

8. In patent violation of its duties and the privacy rights of patients, Defendants enabled such third parties, including Facebook, to intercept and procure confidential patient information and Personal

[2] Defendants' Pixel is a computer code utilized for marketing purposes by enabling organizations to measure activity and enhance consumers' or customers' experiences on web properties. This code is embedded in each page a visitor to the website views and thereby captures Personal Information. The code implemented by Defendants enables third parties, such as Facebook, Google, and others, to procure the Personal Information, furthering the respective business purposes of advertisers and Defendants.

Information, or otherwise assist third parties with intercepting their confidential communications with healthcare providers, despite the fact that Plaintiffs and similarly situated Class Members did not consent, agree, authorize, or otherwise permit Defendants to do so. Defendants did not provide Plaintiffs with any written notice that it discloses its website users' Personal Information to third parties. Nor were Plaintiffs given the option of opting out of such disclosures.

9. Plaintiffs and Class Members relied upon Defendants to maintain the security and privacy of the Personal Information they entrusted to Defendants, and have a reasonable expectation and a right to expect that Defendants would and must comply at all times material with their obligations to keep the Personal Information of Plaintiffs and the Class Members secure and safe from unauthorized access and disclosure.

10. Defendants knowingly implemented and configured tracking code, such as the Facebook Pixel, to disclose the identities and communications of its patients to Facebook and third parties. Defendants implemented the tracking code on its website, all the while with the knowledge and intent to specifically identify their patients to Facebook and third parties alongside their protected health information and geographic location, in direct and patent violation and disregard of the rights of Plaintiffs and Class Members. Defendants' conduct was intentional, willful, reckless, and/or negligent, and constitutes a patent breach of Defendants' own stated privacy policy. As a result, Plaintiffs' and Class Members' Personal Information was compromised through disclosure to Meta/Facebook, and other unknown and unauthorized third parties.[3]

11. Plaintiffs bring this action on behalf of all persons whose Personal Information was accessed and intercepted the Pixel and thus procured or intercepted by third parties, including Facebook and Google, as a result of Defendants' actions.

12. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals who are Class Members, and further seeks remedies that include, but are not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs, as well as injunctive and equitable relief to prevent future injury on behalf of themselves and the putative class.

[3] Meta Platforms, Inc., ("Meta" is the parent company of Facebook)

II. PARTIES

Plaintiffs

13. Plaintiff Steven Beltran is, and at all times mentioned herein was, a resident of the state of California, Los Angeles County, residing in Inglewood. Plaintiff Beltran purchased and received healthcare related services from Defendants and provided Personal Information that was collected by Defendants as a consequence of Plaintiff's use of the Cedars-Sinai website and/or Cedars-Sinai mobile app. Plaintiff Beltran has been a Facebook user since approximately 2011.

14. Plaintiff Lisa Reingold is, and at all times mentioned herein was, a resident of the state of California, Los Angeles County, residing in Aliso Viejo. Plaintiff Reingold purchased and received healthcare related services from Defendants and provided Personal Information that was collected by Defendants as a consequence of Plaintiff's use of the Cedars-Sinai website and/or Cedars-Sinai mobile app. Plaintiff Reingold has been a Facebook user since approximately 2007.

Defendants

15. Defendant Cedars-Sinai Health System is a registered non-profit that provides medical services, including hospital care, primary care, and outpatient care. Cedars-Sinai Health System now serves more than one million patients per year at more than forty locations throughout Southern California, from Westlake Village to Anaheim. Cedars-Sinai Health System is a subsidiary of Defendant Cedars-Sinai Medical Center. Cedars-Sinai Health System is headquartered in Los Angeles County.

16. Defendant Cedars-Sinai Medical Center is a private healthcare organization headquartered in Los Angeles County, and operating a hospital located at 8700 Gracie Allen Drive, Los Angeles, California. Cedars-Sinai Medical Center is the parent of Cedars-Sinai Health System.

17. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown. Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

III. JURISDICTION AND VENUE

18. This Court has jurisdiction over this action pursuant to California Code of Civil Procedure § 410.10, because the total amount of damages to Plaintiffs and the Class exceed $25,000, but the damages suffered by Plaintiffs do not exceed $75,000 on an individual basis.

19. This action is a class action brought pursuant to California Code of Civil Procedure § 382 and, as noted above, because Plaintiffs' claims exceed the jurisdictional minimum of this court, the court has jurisdiction over Plaintiffs' claims.

20. Plaintiffs allege that more than two-thirds of the Class defined herein are citizens of the State of California.

21. Venue is proper in this Court because Defendants are authorized to conduct business within this County and are located in this County.

IV. FACTUAL ALLEGATIONS

Types of Personally Identifiable Patient Information and Healthcare Information that Defendants and Enable Third Parties, such as Facebook and Google, to Procure and Intercept

22. Personally identifiable patient information and personal health information that Defendants enable third parties such as Facebook and Google to procure, access, intercept, and transmit whenever a patient uses the Cedars-Sinai website or application includes, but is not limited to, patient Facebook ID; dates, times, and/or locations of scheduled appointments; patients' proximity to a Cedars-Sinai location; information about patients' medical providers; and the type of appointment or procedure sought (collectively "Personal Information").

23. Plaintiffs are informed and believe and thereon allege that more information was disclosed to Meta/Facebook, Google, and others during the period in which data was submitted to Meta as a result of Defendants' implementation of the Pixel.

24. Through use of the Pixel, Defendants intercept, share, and enable the interception of Plaintiffs' and Class Members' identities and online activity, including personal information and search results related to their private medical treatment. While Defendants were capable of configuring this

tracking software to limit the information that it communicated to third parties, they did not do so and willfully and intentionally configured the Pixel to disseminate patients' Personal Information to third parties, including Facebook, and other similar entities, placing their own business interests and profits ahead of the privacy rights of its patients or above the law.

25. All the while, as Defendants were knowingly violating law and statute, breaching patients' confidentiality, Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendants to disclose their Personal Information and assist with procuring or intercepting their communications. Plaintiffs were never provided with any written notice that Defendants disclose patients' protected health information, nor were they provided any means of opting out of such disclosures. Defendants nonetheless knowingly disclosed Plaintiffs' protected health information to Meta, Facebook, Google, and other unauthorized entities.

26. Plaintiffs and Class Members relied on Defendants to keep their Personal Information confidential and securely maintained, to use this information for their own legitimate healthcare purposes only, and to make only authorized disclosures of this information.

27. Plaintiffs are lawfully entitled to privacy in their protected health information and confidential communications. Defendants knowingly deprived Plaintiffs and Class Members of their privacy rights by its aforesaid conduct without notifying Plaintiffs and Class Members, and without obtaining their express written consent.

Healthcare Patients Have a Reasonable Expectation of Privacy in Their Interactions with Healthcare Websites, Including Defendants'

28. Users of websites related to the provision of healthcare reasonably expect that the information they provide via said websites will not be shared without their affirmative consent. Individual freedom from unauthorized or unwarranted intrusion into the privacy of one's health information is highly valued and the confidentiality of one's health information is viewed as a sacred right.

29. The right of privacy is also viewed as a sacred right. Reflecting its importance, California has adopted privacy laws that prohibit and render unlawful unauthorized interception or recording of

confidential communications, which necessarily includes the unlawful interception, recording, use, or transfer personal health care information.

30. The right of privacy is further guaranteed by Article I, Section I of the California Constitution, which provides:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and ***privacy***"

(Emphasis added).

31. The phrase "and ***privacy***" was added in 1972. The legislative intent in doing so was to curb business' control over the unauthorized collection and use of consumers' personal information. The legislative record states:

> The right of privacy is the right to be left alone… it ***prevents*** government and ***business interests from collecting and stockpiling unnecessary information about us*** and from misusing information gathered for one purpose in order to serve other purposes in order to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and to personal freedom.

(Emphasis provided).[4]

32. Various studies regarding the collection of consumers' personal data confirm that the surreptitious taking of user data – and herein especially confidential health related information – violates expectations of privacy that have been established as general social norms.

33. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

34. A study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same

[4] Ballot Pamphlet, Proposed Stats. & Amends. to Cal. Const. With Arguments to Voters, Gen. Election *26 (Nov. 7, 1972).

percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[5]

35. Moreover, according to a study by Pew Research Center of Americans, harbor concern about how data is collected about them by companies.[6] Healthcare patients – including Plaintiffs – have a legitimate and reasonable expectation that their personal identifying information and personal health information shall be kept private and confidential by their healthcare organizations and providers, and not shared, disclosed, secreted, sold, or monetized by them, or with the participation of third parties, without their knowing, informed, and express consent. This protection regarding such patient information is sacrosanct.

The Cedars-Sinai Privacy Policy and Representations to Patients

36. Defendants provide health care services, including hospital services, inpatient and outpatient care, and other medical services at more than forty locations throughout the Los Angeles basin and surrounding areas. Defendants encouraged patients, such as Plaintiffs and Class Members, to utilize the Cedars-Sinai website, www.cedars-sinai.org, as well as its affiliated mobile app and the MyCS-Link portal, which allows for the scheduling of appointments or procedures, communications with their healthcare providers, review of medical histories and lab results, view and pay bills, and perform other healthcare focused communications.

37. Plaintiffs and Class members paid for and received health-related products or other services from Defendants, and thereby entrusted Defendants with their PII/PHI

38. Plaintiffs and Class Members had a reasonable expectation that Defendants' healthcare business was keeping their Personal Information confidential and securely maintained, would only use this

---

[5] Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds, Consumer Reports (May 11, 2017), https://www.consumerreports.org/ consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[6] Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information, Pew Research Center, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/.

information for their own healthcare, and would not make disclosures of this information without their express authorization.

39. Defendants maintained the PHI/PII and financial information of Plaintiffs and the members of the Class, respecting which it had a duty to adequately secure from unauthorized disclosure.

40. In securing such information as a condition of forming a relationship with Plaintiffs and Class Members, Defendants assumed legal and equitable duties. Additionally, Defendants knew and should have known that they were responsible for protecting such Personal Information from unauthorized disclosure.

41. Defendants were aware at all times material of the fact that given their maintenance of such PII and/or PHI and its knowledge of such risk and its duties, Defendants were responsible for safeguarding the Personal Information in their possession with respect to each Plaintiff and Class Member.

42. At all times material, the Pixel and tracking software code that Defendants installed on the Cedars-Sinai website and the My CS-Link portal tracked users as they navigated through the website and applications, effectively recording which pages are visited, items accessed or clicked, specific medical information users enter such as their search queries and other personal information. Once embedded into Defendants' website, the Pixel or other code transmitted all the information it received to third parties, such as Facebook and Google, thereby enabling them to procure healthcare related and other confidential and Personal Information. These third parties procured, accessed, and intercepted such information without Plaintiffs' and Class Members' consent.

43. Defendants encouraged Plaintiffs and the members of the Class to use these digital tools, promoting the convenience, functionality, and security of the platforms. Defendants promised its patients that "My CS-Link is a secure online health management tool that connects you to your personal health information, view doctor messages, lab results, appointments, billing and more." Defendants further highlighted the benefits of My CS-Link, noting that using it would allow patients to: "Communicate with your physician[;]" "Book and request appointments[;]" "Pay your bill and view your billing history[;]}

"View lab results securely online[;]" "Access your medical records[;]" "Read your doctor's notes[;]" and "Manage your family's health[.]"[7]

44. Defendants' "Joint Notice of Privacy Practices" (the "Joint Notice") covers "the organizations that make up the Cedars-Sinai Affiliated Covered Entity (ACE)."[8] The Joint Notice, last revised on July 1, 2022, provides that information collected from patients can be shared "to promote the joint operations of the participating entities." But said sharing is limited to "[t]he organizations and health professionals participating in an organized healthcare arrangement (OHCA) with Cedars-Sinai ACE entities." According to the Joint Notice, these OHCA participants include:

- Cedars-Sinai ACE entities
- The medical staffs of Cedars-Sinai Medical Center, Cedars-Sinai Marina del Rey Hospital, Torrance Memorial Medical Center and Huntington Hospital
- Affiliated medical groups, professional corporations, independent physicians and allied health professionals contracting with Cedars-Sinai ACE entities to provide services at Cedars-Sinai facilities, unless such healthcare providers give you their own notice of privacy practices that describes how they will protect your medical information[9]

45. Defendants' Joint Notice pertains to any personal information provided to Defendants. It also applies to and any personal information that Defendants collect from other sources. It does not permit Defendants to use and disclose Plaintiffs' and Class Members' Personal Information for marketing purposes without written permission.

46. The Joint Notice assures patients that "[w]e are required by law to maintain the privacy and security of your protected health information."[10] The Joint Notice further assures patients that: "We will

---

[7] https://www.marinahospital.com/portal, last visited on February 21, 2023.

[8] https://www.cedars-sinai.org/content/dam/cedars-sinai/patients/resources-and-patients/patient-privacy/documents/joint-notice-of-privacy-practices.pdf, last visited on February 21, 2023.

[9] *Id.*

[10] *Id.*

not use or share your information other than as described here, unless you tell us in writing we can. If you tell us we can, you can change your mind at any time. Let us know in writing if you change your mind."[11]

47. Nevertheless, Defendants violated their own Joint Notice by unlawfully disclosing Plaintiffs' and Class Members' Personal Information to Facebook/Meta, Google, and other third parties, and misrepresented that it would preserve the confidentiality of their Personal Information and the anonymity of their identities.

48. In addition to their own Joint Notice, Defendants knew and should have known that, HIPAA establishes national minimum standards for the protection of individuals' medical records and other personal health information. HIPAA, generally, applies to health plans/insurers, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, and sets minimum standards for Defendants' maintenance of Plaintiffs' and Class Members' Personal Information. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendants to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization.

49. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

Defendants' Conduct Respecting Third Party Facebook and Others in Violation of Patients' Rights to Privacy and Confidentiality

50. Defendants' conduct enabling Facebook and other third parties to access, intercept, procure, or use patients' Personal Information violates Plaintiffs' and Class Members' rights of privacy and confidentiality. Defendants' conduct violates HIPAA, particularly since it enables or allows third parties to access and procure confidential medical information and patient identifying information. Facebook's

[11] *Id.*

interaction with Defendants', Facebook's, and Google's users and consumers who are patients of Defendants, illustrates the highly intrusive nature of this conduct and third party relationship.

51. By way of example and background, whenever healthcare consumers initiate a Facebook account, they legally agree to its Terms, Data Policy, and Cookie Policy via a checkbox on the sign-up page. These Terms, Data, and Cookie Policies are binding upon Facebook and its users. Facebook's Data Policy states that it "requires" businesses that use the Meta Pixel "to have lawful rights to collect, use, and share your data before providing any data to [Facebook],"[12] However, Facebook does not verify that the businesses using Meta Pixel have obtained the requisite consent to share Plaintiffs' and Class Members' information. As a result, the Meta Pixel is made available to any willing business or publisher regardless of the nature of their business and, in turn, since Plaintiffs and similarly situated Class Members did not consent to or authorize Defendants' enabling Facebook to procure, access, or intercept their Personal Information, Facebook's Meta Pixel contract with Defendants failed to and did not comply with HIPAA.

52. In 2021 alone, Facebook generated $117 billion in revenue, about 97% which was from selling advertising space. In order to sell advertising space and generate revenue, Facebook highlights its ability to target users, which it effectively targets user activity both on and off its site. Facebook compiles information it procures or intercepts into a generalized dataset called "Core Audiences," that advertisers use to apply highly specific filters and parameters for their targeted advertisements.

53. Advertisers in turn build so-called "Custom Audiences" and so-called "Lookalike Audiences" enabling them to reach new consumers and target existing customers directly. Facebook's business tools – bits of code that advertisers can integrate into their website, mobile applications, and servers – enable Facebook to intercept and collect user activity on those platforms. Its business tools enable business partners, including advertisers and others to integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services.

54. Defendants implemented the Facebook Pixel on the Cedars-Sinai digital platforms. The Pixel is a piece of code Facebook offers to advertisers, like Defendants, to integrate into their website. The

[12] See https://www.facebook.com/privacy/policy/version/20220104/.

Facebook Pixel tracks the people and type of actions they take. When a user accesses a website hosting the Facebook Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers. This second, secret transmission contains the original request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent 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 Defendants' websites – Defendants' own code, and Facebook's embedded code. After collecting and intercepting user data and information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

55. Defendants transmit a patient's website activity data to Facebook. Upon doing so the patient's personally identifiable information is disclosed, including their Facebook ID ("FID"), which is a unique identifier Facebook assigns to each user that allows anyone to look up the user's Facebook profile and name. Facebook can easily identify any individual on its Facebook platform with only their unique FID. Any ordinary person who comes into possession of an FID can do likewise, and can connect to the corresponding Facebook profile and the persons' real world identity. A user who accesses Defendants' digital platforms while logged into Facebook will transmit the user cookie to Facebook, which contains that user's unencrypted Facebook ID.

Defendants' Unauthorized Sharing of Personal Information is a Violation of HIPAA

56. Companies in healthcare related business and services such as Defendants are bound by the HIPAA Privacy Rule, 45 CFR §§ 160, 164, which protects all "*"individually identifiable health information,"* or PHI "held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral." PHI includes:

> . . . information that is a subset of health information, including demographic information collected from an individual, and:
>
> (1) Is created or received by a healthcare provider, health plan, employer, or health care clearinghouse; and
>
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

> (i) That identifies the individual; or
>
> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

45 CFR § 160.103. The privacy rule requires that covered entities, including healthcare providers like Defendants, provide sufficient safeguards to protect the privacy of the PHI entrusted to them by patients.

57. HIPAA establishes national minimum standards for the protection of individuals' medical records and other personal health information. HIPAA, generally, applies to health plans/insurers, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, and sets minimum standards for Defendants' maintenance of Plaintiffs' and Class Members' PHI/PII. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendants to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also establishes a series of rights over Plaintiffs' and Class Members' PHI/PII, including rights to examine and obtain copies of their health records, and to request corrections thereto.

58. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

V. CLASS ALLEGATIONS

59. Pursuant to California Code of Civil Procedure § 382, Plaintiffs bring this action on behalf of themselves and a class of similarly situated individuals (the "Class"). The Class is defined as all California citizens who had their Personal Information and/or protected health information disclosed to Facebook through implementation of the Pixel or similar software code.

60. The Class Period is defined as beginning with the date established by the Court's determination of any applicable statute of limitations and after consideration of any tolling, concealment, or accrual issues. The Class Period is defined as ending with the the date of entry of judgment in this action.

61. Excluded from the Class are Defendants, any entity in which Defendants have a controlling interest, Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

62. **Numerosity/Ascertainability**: While the exact number of members of the Class is unknown at this time, Plaintiffs are informed and believe and thereupon allege that the number of persons affected by Defendants' installation of the Facebook Pixel is in the tens, if not hundreds of thousands, making joinder of each individual Class Member impracticable. Ultimately, members of the Class will be easily identified through Defendant' records as well as those of third parties such as Meta/Facebook and Google.

63. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether and to what extent Defendants had a duty to protect Plaintiffs' and Class Members' Personal Information;

b. Whether Defendants had duties not to disclose the Plaintiffs' and Class Members' Personal Information to unauthorized third parties;

c. Whether Defendants had duties not to use Plaintiffs' and Class Members' Personal Information for non-healthcare purposes;

d. Whether Defendants had duties not to use Plaintiffs' and Class Members' Personal Information for unauthorized purposes;

e. Whether Defendants failed to adequately safeguard Plaintiffs' and Class Members' Personal Information;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their Personal Information had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their Personal Information had been compromised;

h. Whether Defendants failed to properly implement and configure the tracking software on its digital platforms to prevent the disclosure of information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur; and

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiffs' and Class Members' Personal Information.

VI. CAUSES OF ACTIONS

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

64. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

65. Plaintiffs and Class Members were required to submit Personal Information to healthcare providers, including Defendants, in order to obtain insurance coverage and/or to receive healthcare services.

66. Defendants knew, or should have known, of the risks and responsibilities inherent in collecting and storing the Personal Information of Plaintiffs and Class Members.

67. As described above, Defendants owed duties of care to Plaintiffs and Class Members whose Personal Information had been entrusted to Defendants.

68. Defendants breached their duties to Plaintiffs and Class Members by failing to secure their Personal Information from unauthorized disclosure to third parties.

69. Defendants acted with wanton disregard for the security of Plaintiffs and Class Members' Personal Information.

70. A "special relationship" exists between Defendants and the Plaintiffs and Class Members. Defendants entered into a "special relationship" with Plaintiffs and Class Members because they collected and/or stored the Personal Information of Plaintiffs and the Class Members.

71. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiffs and the Class Members, Plaintiffs and the Class Members would not have been injured.

72. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known they were failing to meet their duties, and that Defendants' breach would of such duties cause Plaintiffs and Class Members to experience the foreseeable harms associated with the unauthorized exposure of their Personal Information.

73. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II

Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

74. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

75. Pursuant to HIPAA (42 U.S.C. §1302d *et. seq*.), Defendants had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Personal Information.

76. Defendants breached their duties to Plaintiffs and Class Members under HIPAA (42 U.S.C. § 1302d *et. seq.*), by failing to implement reasonable safeguards to protect Plaintiffs' and Class Members' Personal Information, *i.e.,* by affirmatively sharing Plaintiffs' Personal Information, without Plaintiffs' authorization, with third parties.

77. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

78. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

79. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach of those duties would cause Plaintiffs and

Class Members to experience the foreseeable harms associated with the unauthorized sharing of their Personal Information.

80. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III

Breach of Implied Contract
(On behalf of Plaintiffs and the Class)

81. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

82. Plaintiffs and Class members entered into an implied contract with Defendants when they obtained or purchased healthcare related services from Defendants and/or their affiliated healthcare providers, and for which they provided their Personal Information. The Personal Information provided by Class Members that was collected and stored by Defendants was governed by and subject to privacy duties and policies.

83. Defendants implicitly and/or expressly agreed and were under a duty to safeguard and protect the Personal Information of Plaintiffs and Class Members from disclosure.

84. Plaintiffs and Class members entered into the implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with industry standards. Plaintiffs and Class members believed that Defendants would use part of the monies paid to Defendants under the implied contracts to fund adequate and reasonable data security practices.

85. Plaintiffs and Class members would not have obtained healthcare services from Defendants or their affiliated healthcare providers or entrusted their Personal Information which was provided to and stored by Defendants in the absence of the implied contract or implied terms between them and Defendants and its affiliated healthcare providers. The safeguarding of the Personal Information of Plaintiffs and Class Members was critical to realize the intent of the parties.

86. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

87. Defendants breached their implied contracts with Plaintiffs and Class members to protect their Personal Information when Defendants (1) affirmatively inserted the Pixel or similar software tracking code in websites and mobile apps provided by Defendants to Plaintiffs and the Class; (2) disclosed the personal information collected via the Pixel or other tracking code to unauthorized third parties; and (3) failed to notify Plaintiffs and the Class that Defendants were so doing.

88. As a direct and proximate result of Defendants' breaches of implied contract, Plaintiffs and Class members sustained actual losses and damages as described in detail above, and are also entitled to recover nominal damages.

COUNT IV

Breach of Implied Covenant of Good Faith and Fair Dealing (On Behalf of Plaintiffs and the Class)

89. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

90. Plaintiffs and Class Members entered into valid, binding, and enforceable express or implied contracts with Defendants, as alleged above.

91. The contracts respecting which Plaintiffs and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendants would act fairly and in good faith in carrying out their contractual obligations to take reasonable measures to protect Plaintiffs' Personal Information from unauthorized disclosure and to comply with state laws and regulations.

92. A "special relationship" exists between Defendants and the Plaintiffs and Class Members. Defendants entered into a "special relationship" with Plaintiffs and Class Members who sought medical services or treatment at Cedars-Sinai affiliated facilities and, in doing so, entrusted Defendants, pursuant to their requirements and Joint Notice of Privacy Practices, with their Personal Information.

93. Despite this special relationship with Plaintiffs, Defendants did not act in good faith and with fair dealing to protect Plaintiffs' and Class Members' Personal Information.

94. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Defendants.

95. Defendants' failure to act in good faith in complying with the contracts denied Plaintiffs and Class Members the full benefit of their bargain, and instead they received healthcare and related services that were less valuable than what they paid for and less valuable than their reasonable expectations.

96. Accordingly, Plaintiffs and Class Members have been injured as a result of Defendants' breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT V

Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

97. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations as if fully set forth herein.

98. In light of the special relationship between Defendants and Plaintiffs and Class Members, whereby Defendants became guardian of Plaintiffs and Class Members' Personal Information, Defendants became a fiduciary by its undertaking and guardianship of the Personal Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs and Class Members' Personal Information; (2) to timely notify Plaintiffs and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and do store.

99. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship with its patients, in particular, to keep secure their Personal Information from disclosure without authorization from Plaintiffs and the Class Members.

100. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to notify and/or warn Plaintiffs and Class Members that Defendants were sharing their Personal Information with third parties.

101. Defendants breached their fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Personal Information.

102. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the compromise and sharing of their Personal Information; and (ii) the diminished value of the services they received.

103. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
Breach of Duty
(On behalf of Plaintiffs and the Class)

104. Plaintiffs, on behalf of the Class, re-allege and incorporate the above allegations by reference.

105. Defendants accepted the special confidence placed in them by Plaintiffs and Class Members. There was an understanding between the parties that healthcare service provider Defendants would act for the benefit of Plaintiffs and Class Members in preserving the confidentiality of their Personal Information.

106. Defendants became the guardian of Plaintiffs' and Class Members' Personal Information and accepted a fiduciary duty to act primarily for the benefit of its patients, including Plaintiffs and the Class Members, including safeguarding Plaintiffs' and the Class Members' Personal Information.

107. Defendants' fiduciary duty to act for the benefit of Plaintiffs and Class Members pertains as well to matters within the scope of Defendants' medical relationship with its patients, in particular, to keep secure the Personal Information of those patients.

108. Defendants breached their fiduciary duties to Plaintiffs and Class Members by (a) sharing their Personal Information with third parties without authorization; (b) by failing to notify Plaintiffs and the Class Members that Defendants were doing so; and (c) by otherwise failing to safeguard Plaintiffs' and the Class Members' Personal Information.

109. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and/or Class Members have suffered and/or will suffer injury, including but not limited to: (a) the

compromise of their Personal Information; and (b) the diminished value of the services they received as a result of Defendants' unauthorized sharing of Plaintiffs' and Class Members' Personal Information.

110. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VII
Violation of The California Invasion of Privacy Act ("CIPA")
California Penal Code §§ 630, 631, and 632 *et. seq.*
(On Behalf of Plaintiffs and the Class)

111. Plaintiffs, on behalf of the Class, re-allege all of the foregoing allegations as if fully set forth herein.

112. The California Invasion of Privacy Act 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. The Act bars, and establishes penalties for both the interception and recording of private communications.

113. Cal. Penal Code § 631(a) provides for the imposition of a fine of up to $2,500 for:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who 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 . . . .

114. Cal. Penal Code § 632(a) provides, in pertinent part:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the

> parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars . . . .

115. A defendant must show it had the consent of all parties to a communication.

116. Defendants, who maintain their principal places of business in California; implemented and effectuated the Pixel tracking technology to intercept, track, record, store, transmit, and exploit the aforesaid Personal Information while they were engaging in the provision of healthcare services to California consumers.

117. At all relevant times, Defendants' conduct and communications were without authorization and informed consent from the Plaintiffs.

118. The Pixel implemented by Defendants and related code constitute an "electronic amplifying or recording device" under the CIPA, the data Pixel collects is exploited for pecuniary gain, and the Personal Information constitutes "confidential communications." Plaintiffs and Class members had, at all times material, an objectively reasonable expectation of privacy and confidentiality of their Personal Information relating to healthcare services.

119. Plaintiffs have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personally identifiable information.

120. Pursuant to California Penal Code § 637.2, Plaintiffs have been injured by the violations of California Penal Code § 632, *et seq.*, and seeks damages for the greater of $5,000 or three times the amount of actual damages, for each and every instance of violation apiece, and as to Plaintiffs and each Class Member, each of them individually, as well as injunctive relief.

COUNT VIII
Violation of the California Confidentiality of Medical Information Act ("CMIA") Section 56.10 (On Behalf of Plaintiffs and the Class)

121. Plaintiffs, on behalf of the Class, re-allege all of the foregoing allegations as if fully set forth herein.

122. Pursuant to the California Confidentiality of Medical Information Act § 56.10 ("CMIA"), health care providers are prohibited from disclosing their patients' medical information and information

relating to their patients without a patient's authorization. As defined by the CMIA, 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..."

123. Plaintiffs and the members of the Class are each patients, and Defendants are health care providers pursuant to the CMIA, as health care providers, Defendants are obligated to comply with the requirements of the CMIA.

124. As set for the above, the Pixel developed by Facebook and implemented by Defendants provides sufficient personal information and data so as to identify consumers through the collection, sharing, and transmission of, *inter alia*, Facebook IDs coupled with patients' medical conditions, medical concerns, treatment patients sought by patients, scheduling of doctor appointments, and other information.

125. This information is derived from Defendants' provision of health care services to Plaintiffs and the Class, thus, it constitutes medical information pursuant to the CMIA.

126. As set forth above, Defendants fail to get the permission or other valid authorization of Plaintiffs and the Class for disclosure of this medical information.

127. As set forth in CMIA § 56.11, a valid authorization for disclosure of medical information must: (1) be "[c]learly 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) be signed and dated by the patient or his representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date after which the authorization expires. Accordingly, the information set forth in Cedars-Sinai's Joint Statement does not qualify as a valid authorization.

128. On these facts, Defendants are violating the CMIA through their disclosure of the medical information of Plaintiffs and the Class without valid authorization.

COUNT IX
Invasion of Privacy Under California's Constitution
(On Behalf of Plaintiffs and the Class)

129. Plaintiffs, on behalf of the Class, re-allege all of the foregoing allegations as if fully set forth herein.

130. Plaintiffs and the Members of the Class have an interest in protecting and preventing the unauthorized sharing of their Personal Information, including their medical information.

131. Plaintiffs and the members of the Class have a further interest in being able to interact with their healthcare providers in a manner that guarantees the confidentiality of the information shared with their health care providers.

132. Plaintiffs and the members of the Class have a further interest in being able to communicate online without fear of their communications being wiretapped or otherwise illicitly shared without their knowledge and authorization.

133. Plaintiffs and Class Members did not authorize Cedars-Sinai to record and transmit Plaintiffs' and Class Members' Personal Information, including medical information.

134. Defendants' collection and sharing, without authorization, of Plaintiffs' and Class Members' Personal Information constitutes a serious breach of the Plaintiffs' and the Class Members' respective rights to privacy.

135. Plaintiffs and the members of the Class seek all available relief for Defendants' invasion of their privacy.

COUNT X
Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(On Behalf of Plaintiffs and the Class)

136. Plaintiffs, on behalf of the Class, re-allege all of the foregoing allegations as if fully set forth herein.

137. Defendants are each a "person" as that defined by Cal. Bus. & Prof. Code § 17201.

138. Defendants violated the California Unfair Competition Law ("UCL"), §§ 17200, *et seq*., by engaging in unlawful, unfair, and deceptive business acts and practices as alleged above by using, and

exploiting or divulging to third persons the private confidential financial information of Plaintiffs and class members, and without the knowledge of Plaintiffs and the Class intercepting, collecting, using, and exploiting the private confidential information of Plaintiffs and the Class.

139. Defendants engaged in unlawful business practices through its numerous violations of law, including violations of California Penal Code §§ 630, 631, and 632, *et seq*.

140. Defendants' aforesaid surreptitious conduct, deception, and omissions respecting Plaintiffs and the Class were material because they were likely to deceive reasonable individuals about Defendants' adherence to their own stated and publicized privacy policies and procedures and their reasonable expectations of the privacy of their Personal Information.

141. Defendants' conduct, as described above, was unfair in that it prevented the making of fully informed decisions by consumers, such as Plaintiffs and the members of the Class, regarding which health care providers to use and prevented Plaintiffs and the Class from making fully informed decisions regarding the communication of Personal Information to their healthcare providers.

142. Defendants intended to deceive or mislead Plaintiffs and the Class, and induced them.

143. Defendants' actions constituted intentional, knowing, and malicious violations of the UCL in reckless disregard of the rights of Plaintiffs and the Class.

144. As a direct and proximate result of Defendants' violations of the UCL, Plaintiffs and the Class sustained actual losses and damages as described herein.

145. Plaintiffs and the Class seek restitution, injunctive relief, and other and further relief as the Court may deem just and proper. To the extent any of these remedies are equitable, Plaintiffs seek them in the alternative to any adequate remedy at law they may have.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, prays for relief and judgment against Defendants as follows:

A. certifying the Class pursuant to Section 382 of the Code of Civil Procedure, appointing Plaintiffs as representatives of the Class, and designating Plaintiffs' counsel as Class Counsel;

B. declaring that Defendants' conduct violates the laws referenced herein;

C. finding in favor of Plaintiffs and the Class on all counts asserted herein;

D. awarding Plaintiffs and the Class compensatory damages and actual damages, trebled, in an amount exceeding $5,000,000, to be determined by proof;

E. awarding Plaintiffs and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiffs and the Class punitive damages;

G. awarding Plaintiffs and the Class civil penalties;

H. granting Plaintiffs and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendants from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiffs and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiffs and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: February 23, 2022

Respectfully submitted,

BARRACK, RODOS & BACINE

/s/ Samuel M. Ward

SAMUEL M. WARD (216562)
600 West Broadway, Suite 900
San Diego, CA 92101
sbasser@barrack.com

sward@barrack.com
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

EMERSON FIRM, PLLC
JOHN G. EMERSON*
2500 Wilcrest, Suite 300
Houston, TX 77042
jemerson@emersonfirm.com
Telephone: (800) 551-8649
Facsimile: (501) 286-4659

Counsel for Plaintiffs

**Pro Hac Vice* application to be filed