POTTER HANDY LLP
Mark D. Potter (SBN 166317)
mark@potterhandy.com
James M. Treglio (SBN 228077)
jimt@potterhandy.com
100 Pine St., Ste 1250
San Francisco, CA 94111
Tel: (415) 534-1911
Fax: (888) 422-5191

Attorneys for Plaintiffs Christopher Newton, Christa Vital, Scott Schutza, on behalf of themselves and all others similarly situated,

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ALAMEDA

CHRISTOPHER NEWTON, CHRISTA VITAL, SCOTT SCHUTZA, on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

KAISER FOUNDATION HEALTH PLAN, INC., a California Corporation; META PLATFORMS, INC., a Delaware Corporation; GOOGLE LLC, a Delaware Limited Liability Company; and DOES 1 through 100, inclusive,

Defendants.

CASE NO. 24CV073453

FIRST AMENDED CLASS ACTION COMPLAINT

CLASS COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF (FOR VIOLATIONS OF:

(1) THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CIVIL CODE §§ 56, *ET SEQ*.);
(2) CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §17200, *ET SEQ.;*
(3) NEGLIGENCE;
(4) NEGLIGENCE PER SE;
(5) COMMON LAW INVASION OF PRIVACY – INTRUSION UPON SECLUSION;
(6) CALIFORNIA INVASION OF PRIVACY ACT CAL. PENAL CODE § 631; and
(7) CALIFORNIA INVASION OF PRIVACY ACT CAL. PENAL CODE § 632.

DEMAND FOR JURY TRIAL

Class Representative Plaintiffs Christopher Newton, Christa Vital, and Scott Schutza ("Plaintiffs"), by and through their attorneys, individually and on behalf of others similarly situated, allege upon information and belief as follows:

I.

INTRODUCTION

1. Under the Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.* (hereinafter referred to as the "Act"), Plaintiffs Christopher Newton, Christa Vital, Scott Schutza and all other persons similarly situated, had a right to keep their personal medical information provided to Defendant KAISER FOUNDATION HEALTH PLAN, INC. ("Kaiser"), META PLATFORMS, INC. ("Meta"), and GOOGLE LLC ("Google") (collectively, "Defendants") confidential. The short title of the Act states, "The Legislature hereby finds and declares that persons receiving health care services have a right to expect that the confidentiality of individual identifiable medical information derived by health service providers be reasonably preserved. It is the intention of the Legislature in enacting this act, to provide for the confidentiality of individually identifiable medical information, while permitting certain reasonable and limited uses of that information." The Act specifically provides that "a provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization...." Civil Code. § 56.10(a). The Act further provides that "Every provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall be subject to the remedies ... provided under subdivisions (b) ... of Section 56.36." Civil Code § 56.101(a).

2. Civil Code § 56.36(b) provides Plaintiffs, and all other persons similarly situated, with a private right to bring an action against Defendants for violation of Civil Code § 56.101 by

specifically providing that "[i]n addition to any other remedies available at law, any individual may bring an action against any person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: (1) ... nominal damages of one thousand dollars ($1,000). In order to recover under this paragraph, *it shall not be necessary that the plaintiff suffered or was threatened with actual damages*. (2) The amount of actual damages, if any, sustained by the patient." (Emphasis added.) Here, the release of information to third parties without so much as a subpoena clearly violates the requirements of this statute.

3. This class action is brought on behalf of Plaintiffs and a putative class defined as: "All natural persons in the United States who used the Kaiser Platform and whose communications and/or data were intercepted by Defendants, and who received a Notice of Data Breach in May of 2024." ("the "Class," or the "Class Members").

4. As alleged more fully below, Kaiser created, maintained, preserved, and stored Plaintiffs and the Class members' personal medical information onto Kaiser's computer network, including websites and web applications prior to October 2023. Due to Kaiser's intentional release of information without authorization, there was an unauthorized release of Plaintiffs' and the Class members' confidential medical information that occurred continuously from the time this information was provided by the Class to Kaiser, in violation of Civil Code § 56.101 of the Act.

5. As alleged more fully below, Kaiser created, maintained, preserved, and stored Plaintiffs' and the Class members' confidential medical information which were released to unauthorized persons, without Plaintiffs' and the Class members' prior written authorization. This act of providing unauthorized access to Plaintiffs' and the Class Members' confidential medical information continuously constitutes an unauthorized release of confidential medical information in violation of Civil Code § 56.101 of the Act. Because Civil Code § 56.101 allows for the remedies and penalties provided under Civil Code § 56.36(b), Class Representative Plaintiffs, individually and on behalf of others similarly situated, seek nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1). Additionally, Class Representative Plaintiffs,

individually and on behalf of others similarly situated, seek injunctive relief for unlawful violations of Business and Professions Code §§ 17200, *et seq*.

6. Unbeknownst to Plaintiffs and Class members, Meta and Google's technology was intentionally incorporated on the Kaiser Platform, through which Meta and Google intercepted users' health data and other highly sensitive information. Meta and Google intercepted, at least, users' "IP address, name, information that could indicate you were signed into a Kaiser Permanente account or service, information showing how you interacted with and navigated through our website or mobile applications, and search terms used in the health encyclopedia."

7. This information was not aggregated or deidentified, nor were Meta and Google prohibited from using this information for their own benefit.

8. Plaintiffs provided their information, including health data and PII in connection with obtaining prescriptions and medical appointments, to Kaiser with the expectation that this information would remain confidential and private.

9. Meta and Google's interception of this information without consent constitutes an extreme invasion of Plaintiffs' and Class members' privacy. Given the secret and undisclosed nature of Google and Meta's conduct, additional evidence supporting Plaintiffs' claims, including the full extent of medical information they intercepted, and how they used that information, will be revealed in discovery.

10. Class Representative Plaintiffs do not seek any relief greater than or different from the relief sought for the Class of which Plaintiffs are members. The action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons. Private enforcement is necessary and places a disproportionate financial burden on Class Representative Plaintiffs in relation to Class Representative Plaintiffs' stake in the matter.

II.

JURISDICTION AND VENUE

11. This Court has jurisdiction over this action under California Code of Civil Procedure § 410.10. The aggregated amount of damages incurred by Plaintiffs and the Class exceeds the

$25,000 jurisdictional minimum of this Court. The amount in controversy as to the Plaintiffs individually and each individual Class member does not exceed $75,000, including interest and any pro rata award of attorneys' fees, costs, and damages. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of Civil Procedure §§ 395(a) and 395.5 because Kaiser is registered while all Defendants do business in the State of California and in the County of Alameda. Defendants obtained medical information in the transaction of business in the County of Alameda, which has caused both obligations and liability of Defendants to arise in the County of Alameda.

III.

PARTIES

A. PLAINTIFFS

12. Class Representative Plaintiff Christopher Newton is a resident of California. At all times relevant, Plaintiff was a patient of Kaiser who utilized Kaiser website and web application to receive medical treatment medical treatment from Kaiser, and was a patient, as defined by Civil Code § 56.05(k). Plaintiff's individual identifiable medical information derived by Kaiser in electronic form was in possession of Kaiser, including but not limited to Plaintiff's medical history, mental or physical condition, or treatment, including diagnosis and treatment dates. Such medical information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as Plaintiff's name, date of birth, addresses, medical record number, insurance provider, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals Plaintiff's identity. During this time, Plaintiff also maintained accounts with Meta and Google, using the same device used to access the Kaiser platform to access Meta and Google platforms. However, unbeknownst to Plaintiff, Meta and Google intercepted information, including PII, health data, prescription requests, and other activity across the Kaiser Platform. Plaintiff did not consent to the interception of his data, which was never disclosed and directly contrary to the representations made by Kaiser.

13. Class Representative Plaintiff Christa Vital is a resident of California. At all times relevant, Plaintiff was a patient of Defendant who utilized Defendant's website and web application

to receive medical treatment from Defendant, and was a patient, as defined by Civil Code § 56.05(k). Plaintiff's individual identifiable medical information derived by Defendant in electronic form was in possession of Defendant, including but not limited to Plaintiff's medical history, mental or physical condition, or treatment, including diagnosis and treatment dates. Such medical information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as Plaintiff's name, date of birth, addresses, medical record number, insurance provider, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals Plaintiff's identity. Since receiving treatment at Defendant's facilities, Plaintiff has received numerous solicitations by mail and phone from third parties at an address and number she only provided to Defendant. She has also begun receiving phone call regarding health issues she and her family have sought treatment for. During this time, Plaintiff also maintained accounts with Meta and Google, using the same device used to access the Kaiser platform to access Meta and Google platforms. However, unbeknownst to Plaintiff, Meta and Google intercepted information, including PII, health data, prescription requests, and other activity across the Kaiser Platform. Plaintiff did not consent to the interception of her data, which was never disclosed and directly contrary to the representations made by Kaiser.

14. Class Representative Plaintiff Scott Schutza is a resident of California. At all times relevant, Plaintiff was a patient of Defendant who utilized Defendant's website and web application to receive medical treatment medical treatment from Defendant, and was a patient, as defined by Civil Code § 56.05(k). Plaintiff's individual identifiable medical information derived by Defendant in electronic form was in possession of Defendant, including but not limited to Plaintiff's medical history, mental or physical condition, or treatment, including diagnosis and treatment dates. Such medical information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as Plaintiff's name, date of birth, addresses, medical record number, insurance provider, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals Plaintiff's identity. During this time, Plaintiff also maintained accounts with Meta and

Google, using the same device used to access the Kaiser platform to access Meta and Google platforms. However, unbeknownst to Plaintiff, Meta and Google intercepted information, including PII, health data, prescription requests, and other activity across the Kaiser Platform. Plaintiff did not consent to the interception of his data, which was never disclosed and directly contrary to the representations made by Kaiser.

15. On April 26, 2027, Plaintiffs and the Class were informed through an article on various media outlets, such as Techcrunch that their personal medical information and personal identifying information were disclosed to "third-party advertisers, including Google, Microsoft and X (formerly Twitter)."[1] This information was subsequently confirmed by Kaiser in its filing with the United States Department of Health and Human Services. Subsequently, Plaintiffs received notices from Kaiser that their information was included in the data breach.

B. DEFENDANTS

16. Defendant Kaiser Foundation Health Plan, Inc. is a California corporation, with its principal places of business located at One Kaiser Plaza, Oakland, CA 94612. At all times relevant, Kaiser is a "provider of health care" as defined by Civil Code § 56.05(m). Prior to October 2023, Kaiser created, maintained, preserved, and stored Plaintiffs' and the Class members' individually identifiable medical information onto its computer network, including but not limited to Plaintiffs' and the Class members' medical history, mental or physical condition, or treatment, including diagnosis and treatment dates. Such medical information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as Plaintiffs' and the Class members' names, dates of birth, addresses, medical record numbers, insurance providers, electronic mail addresses, telephone numbers, or social security numbers, or other information that, alone or in combination with other publicly available information, reveals Plaintiffs' and the Class members' identities.

17. Defendant Meta is a Delaware corporation, with its principal places of business located at 1 Meta Way, Menlo Park, CA 94025. Meta at all times knew that the incorporation of its

[1] Whittaker, Zack. "Health insurance giant Kaiser will notify millions of a data breach after sharing patients' data with advertisers," https://techcrunch.com/2024/04/25/kaiser-permanente-health-plan-millions-data-breach/ last accessed on April 26, 2024.

software into the Kaiser Platform would result in its interception of identifiable health information and other sensitive data. Meta, as the creator of its SDK and Meta Pixel, knew that it intercepted each of a user's interactions on the website or mobile application that incorporated this technology. Meta has consistently come under scrutiny for incorporating its technology on websites and applications that involve the transmittal of sensitive data, including health information, yet continues to do so.

18. For instance, in February 2019, the Wall Street Journal published an in-depth analysis of Meta's collection of sensitive health information using its tracking technology from certain mobile applications. These reports led to a subsequent investigation by the Federal Trade Commission, who confirmed that Meta did in fact collect sensitive health information from a popular women's health app, including pregnancy data, between June 2016 to February 2019. It also confirmed that Meta went on to use this information for its own research and development. The New York State Department of Financial Services conducted a similar investigation of Meta and reached a similar conclusion, including finding that Meta did not take sufficient steps or precautions to prevent its interception of this kind of information or its use for commercial purposes.

19. Further, since at least 2016, Meta has allowed granular ad targeting based on sensitive information collected or received about individuals, including relating to at least breast feeding, ethnicities, religious beliefs, and income levels. Despite this, it was not until November 9, 2021, that Meta acknowledged its use of data to target users based on "sensitive" topics, including "health" and how that was problematic. While Meta stated that it would remove this functionality in part, it later clarified that the change was limited to individuals' interactions with "content" on the Facebook platform (i.e., the "Detailed Targeting" option on Facebook) and did not apply to data intercepted through Meta Pixel or SDK or collected through other means. Thus, advertisers were still permitted to use "website custom audiences" and "lookalike" audiences to target users based on the information Meta intercepted through Meta Pixel and its SDK.

20. Further, Meta has acknowledged its interception of sensitive data, including health information, in public statements highlighting its efforts to develop a "Health Terms Integrity System" intended to filter out this type of information and prevent them from entering Meta's

system. However, independent investigations have confirmed these data filtration systems are not successful at preventing the interception of health data. For instance, researchers at The Markup found while investigating the use of the Meta Pixel on abortion-related websites that Meta's purported "filtering" system failed to discard even the most obvious forms of sexual health information, including URLs that included the phrases "post-abortion," "i-think-im-pregnant," and "abortion-pill."

21. Meta's own employees have confirmed the same, admitting that Meta lacks the ability to prevent the collection of sensitive health data or its use in ads. For example, Meta engineers on the ad and business product team wrote in a 2021 privacy overview "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data f or Y purpose.'"

22. Meta did not take any steps to prevent Kaiser from using its technology on the Kaiser Platform or to prevent its interception and use of Kaiser users' sensitive health data—like answers to health questions. As such, Meta's conduct was intentional despite knowing the privacy violations it caused to Plaintiffs and Class members.

23. Defendant Google is a Delaware limited liability company, with its principal places of business located at 1600 Amphitheatre Parkway, Mountain View, CA 94043. Google at all times knew that the incorporation of its software into the Kaiser Platform would result in its interception of identifiable health information and other sensitive data. Google did not take any steps to prevent Kaiser from using its technology on the Kaiser Platform or to prevent its interception and use of Kaiser users' sensitive health data—like answers to health questions. As such, Google's conduct was intentional despite knowing the privacy violations it caused to Plaintiffs and Class members.

C. DOE DEFENDANTS

24. The true names and capacities, whether individual, corporate, associate, or otherwise, of Defendants sued herein as DOES 1 through 100, inclusive, are currently unknown to the Plaintiffs, who therefore sue the Defendants by such fictitious names under the Code of Civil Procedure § 474. Each of the Defendants designated herein as a DOE is legally responsible in some

manner for the unlawful acts referred to herein. Plaintiffs will seek leave of court and/or amend this complaint to reflect the true names and capacities of the Defendants designated hereinafter as DOES 1 through 100 when such identities become known. Any reference made to a named Defendant by specific name or otherwise, individually or plural, is also a reference to the actions or inactions of DOES 1 through 100, inclusive.

D. AGENCY/AIDING AND ABETTING

25. At all times herein mentioned, Defendants, and each of them, were an agent or joint venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

26. Defendants, and each of them, aided and abetted, encouraged and rendered substantial assistance to the other Defendants in breaching their obligations to Plaintiffs and the Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially assist the commissions of these wrongful acts and other wrongdoings complained of, each of the Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals, and wrongdoing.

IV.

FACTUAL ALLEGATIONS

A. The Unauthorized Release

27. On April 26, 2027, Plaintiffs and the Class were informed through an article on Techcrunch and other medica outlets that their personal medical information and personal identifying information were disclosed to "third-party advertisers, including Google, Microsoft and X (formerly Twitter)." [2] ("Notice"). At no point had Plaintiffs and the Class provided any authorization to Kaiser to release any medical records to any person on their behalf. Nor was any

[2] *Id.*

information sought at this time by any third party by way of a subpoena or request for documents in discovery. ("Data Breach").

28. The reports further stated that Kaiser "conducted an investigation that found "certain online technologies, previously installed on its websites and mobile applications, may have transmitted personal information to third-party vendors.""

29. The reports also mentioned "that the data shared with advertisers includes member names and IP addresses, as well as information that could indicate if members were signed into a Kaiser Permanente account or service and how members "interacted with and navigated through the website and mobile applications, and search terms used in the health encyclopedia.""

30. According to the media reports, Kaiser "subsequently removed the tracking code from its websites and mobile apps."

31. Although the reports mentioned that Kaiser "filed a legally required notice with the U.S. government on April 12 but made public on Thursday confirming that 13.4 million residents had information exposed," and "notified California's attorney general of the data breach," Kaiser's spokesperson confirmed that Kaiser has yet to notify the affected individuals. The Notice stated "that the organization would begin notifying 13.4 million affected current and former members and patients who accessed its websites and mobile apps. The notifications will start in May in all markets where Kaiser Permanente operates, the spokesperson said."

32. As such, Plaintiffs are informed and believe that Kaiser regularly gave unrestricted access to third parties to the Personal and Medical Information of Plaintiffs and all Class Members for an undetermined period of time prior to October 2023.

33. On or about May 13, 2024, Kaiser sent email notices to Plaintiffs and the Class ("Email Notice"). The Email Notice stated that "On October 25, 2023, Kaiser Permanente determined that certain online technologies (commonly known as cookies or pixels) installed on our websites and mobile applications may have transmitted personal information to our third-party vendors Google, Microsoft Bing, and X (Twitter) when members and patients accessed our websites or mobile applications. These technologies are sometimes used by organizations to understand how consumers interact with websites and mobile applications."

34. According to the Email Notice, "The information that may have been involved was limited to: IP address, name, information that could indicate you were signed into a Kaiser Permanente account or service, information showing how you interacted with and navigated through our website or mobile applications, and search terms used in the health encyclopedia. Detailed information concerning Kaiser Permanente account credentials (username and password), Social Security numbers, financial account information and credit card numbers were not included in the information involved."

35. With regard to the steps taken by Kaiser with regard to the Data Breach, the Email Notice stated that "We conducted a voluntary internal investigation into the use of these online technologies, and subsequently removed these online technologies from our websites and mobile applications. In addition, Kaiser Permanente has implemented additional measures with the guidance of experts to safeguard against recurrence of this type of incident."

36. Finally, the Email Notice encouraged Plaintiffs and the Class " it is always advisable to remain vigilant against attempts at identity theft or fraud, which includes reviewing online and financial accounts, credit reports, and Explanations of Benefits for suspicious activity. This is a best practice for all individuals. … If you are concerned about identity theft and would like more information on ways to protect yourself, visit the Federal Trade Commission's Identity Theft website at https://www.identitytheft.gov."

37. Yet, despite knowing many patients were in danger, Kaiser did nothing to warn Class Members until almost seven months after the Data Breach occurred. During this time, unauthorized third parties had free reign to surveil and defraud their unsuspecting victims. Kaiser proceeded business as usual without giving class members the information they needed to protect themselves against fraud and identity theft.

38. Moreover, during the time period of the release, Class Members, including the Plaintiffs, began noticing advertisements on social media sites, such as Facebook and Instagram for illnesses that they previously had only disclosed to their physicians. These advertisements clearly indicate that not only was medical information released to third parties, but the information was viewed, and then acted upon.

39. It is apparent from the Email Notice, reports, and subsequent filings with the United States Department of Health and Human Services and the California Attorney General's office, that Kaiser stores the personal medical information of the Class Members and released them to unauthorized third parties.

40. Kaiser failed to adequately safeguard Plaintiffs and Class Members' Personal and Medical Information, allowing unauthorized third parties to access this wealth of priceless information for an undetermined period of time prior to October 2023, and possibly continuing to date, without warning the victims, the Class Members, to be on the lookout.

41. Kaiser failed to spend sufficient resources on making sure that its patients' personal medical information are secure and released only to authorized persons.

42. Kaiser had obligations created by the Health Insurance Portability and Accountability Act ("HIPAA"), the Confidentiality of Medical Information Act ("CMIA"), reasonable industry standards, its own contracts with its patients and employees, common law, and its representations to Plaintiffs and Class members, to keep their Personal and Medical Information confidential and to protect the information from unauthorized access.

43. Plaintiffs and Class members provided their Personal and Medical Information to Kaiser with the reasonable expectation and mutual understanding that it would comply with its obligations to keep such information confidential and secure from unauthorized access.

44. Indeed, as discussed below, Kaiser promised Plaintiffs and Class members that it would do just that.

B. Kaiser Expressly Promised to Protect Personal and Medical Information

45. Kaiser provides all patients, including Plaintiffs and Class members, its Notice of Privacy Practices, which states that:

> II. ABOUT OUR RESPONSIBILITY TO PROTECTYOUR PHI
>
> By law, we must
>
> 1. protect the privacy of your PHI;
> 2. tell you about your rights and our legal duties with respect to your PHI;
> 3. notify you if there is a breach of your unsecured PHI; and

4. tell you about our privacy practices and follow our notice currently in effect.
We take these responsibilities seriously and, have put in place administrative safeguards(such as security awareness training and policies and procedures), technical safeguards(such as encryption and passwords), and physical safeguards (such as locked areas and requiring badges) to protect your PHI and, as in the past, we will continue to take appropriate steps to safeguard the privacy of your PHI.[3]

46. Likewise, Kaiser's Notice of Privacy Practices also states that:

VI. ALL OTHER USES AND DISCLOSURES OFYOUR PHI REQUIRE YOUR PRIOR WRITTENAUTHORIZATION

Except for those uses and disclosures described above, we will not use or disclose your PHI without your written authorization. Some instances in which we may request your authorization for use or disclosure of PHI are:

Marketing:
We may ask for your authorization in order to provide information about products and services that you may be interested in purchasing or using. Note that marketing communications do not include our contacting you with information about treatment alternatives, prescription drugs you are taking or health-related products or services that we offer or that are available only to our health plan enrollees. Marketing also does not include any face-to-face discussions you may have with your providers about products or services.

Sale of PHI:
We may only sell your PHI if we received your prior written authorization to do so.

Psychotherapy Notes:
On rare occasions, we may ask for your authorization to use and disclose "psychotherapy notes". Federal privacy law defines "psychotherapy notes" very specifically to mean notes made by a mental health professional recording conversations during private or group counseling sessions that are maintained separately from the rest of your medical record. Generally, we do not maintain psychotherapy notes, as defined by federal privacy law.

When your authorization is required and you authorize us to use or disclose your PHI for some purpose, you may revoke that authorization by notifying us in writing at any time. Please note that the revocation will not apply to any authorized use or

[3] Kaiser, "Notice of Privacy Practices," Effective Date: September 22, 2023, https://healthy.kaiserpermanente.org/southern-california/privacy-practices , last visited on April 26, 2024.

> disclosure of your PHI that took place before we received your revocation. Also, if you gave your authorization to secure a policy of insurance, including health care coverage from us, you may not be permitted to revoke it until the insurer can no longer contest the policy issued to you or a claim under the policy.[4]

47. Notwithstanding the foregoing assurances and promises, Kaiser failed to protect the Personal and Medical Information of Plaintiffs and other Class members from releasing their information to unauthorized third parties, as conceded by Kaiser in the Notice.

48. If Kaiser truly understood the importance of safeguarding patients' Personal and Medical Information, it would acknowledge its responsibility for the harm it has caused, and would compensate class members, provide long-term protection for Plaintiffs and the Class, agree to Court-ordered and enforceable changes to its policies and procedures, and adopt regular and intensive training to ensure that an unauthorized release like this never happens again.

49. That information is now in the hands unauthorized third parties who will use it if given the chance. In fact, Plaintiff Vital already has begun receiving direct solicitations and advertisements from third parties regarding medical conditions she sought treatment for. Much of this information is unchangeable and loss of control of this information is remarkably dangerous to consumers.

C. Kaiser had an Obligation to Protect Personal and Medical Information under Federal and State Law and the Applicable Standard of Care

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

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

[4] *Id.*

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

53. HIPAA requires Kaiser to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

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

55. HIPAA's Security Rule requires Kaiser to do the following:

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

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

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

d. Ensure compliance by its workforce.

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

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

58. Kaiser was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable

and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

59. In addition to their obligations under federal and state laws, Kaiser owed a duty to Class Members whose Personal and Medical Information was entrusted to Kaiser to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal and Medical Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Kaiser owed a duty to Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its systems, policies, procedures, and the personnel responsible for them, adequately protected the Personal and Medical Information of the Class Members.

60. Kaiser owed a duty to Class Members whose Personal and Medical Information was entrusted to Kaiser to design, maintain, and test its systems, policies, and procedures to ensure that the Personal and Medical Information in Kaiser's possession was adequately secured and protected.

61. Kaiser owed a duty to Class Members whose Personal and Medical Information was entrusted to Kaiser to create and implement reasonable data security practices and procedures to protect the Personal and Medical Information in their possession, including adequately training its employees and others who accessed Personal Information within its computer systems on how to adequately protect Personal and Medical Information.

62. Kaiser owed a duty to Class Members whose Personal and Medical Information was entrusted to Kaiser to implement processes that would detect an unauthorized access in a timely manner.

63. Kaiser owed a duty to Class Members whose Personal and Medical Information was entrusted to Kaiser to act upon data security warnings and alerts in a timely fashion.

64. Kaiser owed a duty to Class Members whose Personal and Medical Information was entrusted to Kaiser to adequately train and supervise its employees to identify and avoid any phishing emails that make it past its email filtering service.

65. Kaiser owed a duty to Class Members whose Personal and Medical Information was entrusted to Kaiser to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal and Medical Information from theft or access by unauthorized third parties because such an inadequacy would be a material fact in the decision to entrust Personal and Medical Information with Kaiser.

66. Kaiser owed a duty to Class Members whose Personal and Medical Information was entrusted to Kaiser to disclose in a timely and accurate manner when an unauthorized access occurred.

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

D. An Unauthorized Release like this Results in Debilitating Losses to Consumers

68. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[5] Unauthorized third parties can leverage Plaintiffs' and Class members' Personal and Medical Information that was obtained in the unauthorized release to commit thousands-indeed, millions-of additional crimes, including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services and government benefits, using Class Members' Personal Information to file fraudulent tax returns, using Class Members' health insurance information to rack up massive medical debts in their names, using Class Members' health information to target them in other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest. Even worse, Class Members could be arrested for crimes identity thieves have committed.

[5] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

69. Personal and Medical Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years.

70. This is not just speculative. As the FTC has reported, if unauthorized third parties get access to Personal and Medical Information, they ***will*** use it.[6]

71. Unauthorized third parties may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information **may continue for years**. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

72. Medical identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more "than identity thefts involving banking and finance, the government and the military, or education."[8]

73. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[9]

74. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI can go from $20 say up to—we've seen $60 or $70

---

[6] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[7] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu (emphasis added).

[8] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

[9] *Id.*

[(referring to prices on dark web marketplaces)]."[10] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[11]

75. As a direct and proximate result of the unauthorized release, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the unauthorized release on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

76. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Personal and Medical Information;

b. Improper disclosure of their Personal and Medical Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal and Medical Information being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the unauthorized release;

f. Loss of privacy suffered as a result of the unauthorized release, including the harm of knowing unauthorized third parties have their Personal and Medical Information and that

[10] ID Experts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, https://www.idexpertscorp.com/knowedge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat

[11] *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from The Global State of Information Security Survey 2015,https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global- state-of-information-security-survey-2015.pdf

fraudsters have already used that information to initiate spam calls to members of the Class;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the unauthorized release;

h. Ascertainable losses in the form of deprivation of the value of customers' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal and Medical Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

77. Moreover, Plaintiffs and Class have an interest in ensuring that their information, which remains in the possession of Kaiser, is protected from further unauthorized release by the implementation of security measures and safeguards.

78. Even if Kaiser would acknowledge the harm caused by the unauthorized release by recommending that Plaintiffs and Class Members review the statements they receive from their healthcare providers and health insurer, any amount of identity theft repair and monitoring is woefully inadequate to protect Plaintiffs and Class members from a lifetime of identity theft risk and worse, it does nothing to reimburse Plaintiffs and Class members for the injuries they have already suffered.

79. All this is made worse because Plaintiffs and the Class Members know that their information is widely shared through these third parties. They have already received solicitations and advertisements for various medical conditions that were previously only disclosed to their physicians on the Kaiser website or web application.

E. Meta's Tracking Technology on the Kaiser Platform

80. Meta is one of the largest advertising companies in the country. To date, Meta generates nearly 98% of its revenue through advertising bringing in a grand total of $114.93 billion.

81. Meta's advertising business began back in 2007 with the creation of "Facebook Ads," which was marketed as a "completely new way of advertising online" that would allow "advertisers to deliver more tailored and relevant ads."

82. Today, Meta provides advertising on its own platforms, such as Facebook and Instagram, as well as websites outside these apps through the Facebook Audience Network. Facebook alone has more than 3 billion active users.[12]

83. Meta's advertising business has been extremely successful due, in large part, to Meta's ability to target people at a granular level. "Among many possible target audiences, [Meta] offers advertisers," for example, "1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'"

84. Given the highly specific data used to target specific users, it is no surprise that millions of companies and individuals utilize Meta's advertising services. Meta generates substantially all of its revenue from selling advertisement placements:

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	$117.93 billion	$114.93 billion	97.46%
2020	$85.97 billion	$84.17 billion	97.90%
2019	$70.70 billion	$69.66 billion	98.52%
2018	$55.84 billion	$55.01 billion	98.51%

85. One of Meta's most powerful advertising tools is the Meta Pixel, formerly known as the Facebook Pixel, which launched in 2015 and its software development kit (SDK).

86. Meta touted the Meta Pixel as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website." According to Meta, to use the Meta Pixel an advertiser need only "place a single pixel across [its] entire website to report and optimize for conversions" so that the advertiser could "measure the effectiveness of [its] advertising by understanding the action people take on [its] website." The Meta Pixel is incorporated on 6.7 million websites, including Kaiser's website.

[12] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ last visited on June 9, 2024.

87. The Meta Pixel is a snippet of code embedded on a third-party website that tracks a users' activity as the users navigate through a website. As soon as a user takes any action on a webpage that includes the Meta Pixel, the code embedded in the page re-directs the content of the user's communication to Meta while the exchange of the communication between the user and website provider is still occurring.

88. Through this technology, Meta intercepts each page a user visits, what buttons they click, as well as specific information they input into the website and what they searched. The Meta Pixel sends each of these pieces of information to Meta with other identifiable information, such as the users IP address. Meta stores this data on its own server, in some instances, for years on end.

89. This data is often associated with the individual users' Facebook account. For example, if the user is logged into their Facebook account when the user visits Kaiser's website, Meta receives third party cookies allowing Meta to link the data collected by the Meta Pixel to the specific Facebook user.

90. Meta can also link the data to a specific user through the "Facebook Cookie." The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users, including Facebook users.

91. Lastly, Meta can link user data to individual users through identifying information collected through the Meta Pixel through what Meta calls "Advanced Matching." There are two forms of Advanced Matching: manual matching and automatic matching. Using Manual Advanced Matching the website developer manually sends data to Meta to link users. Using Automatic Advanced Matching, the Meta Pixel scours the data it receives to search for recognizable fields, including name and email address to match users to their Facebook accounts.

92. Importantly, even if the Meta Pixel collects data about a non-Facebook user, Meta still retains and uses the data collected through the Meta Pixel in its analytics and advertising services. These non-users are referred to as having "shadow profiles" with Meta.

93. At the time Plaintiffs used the Kaiser Platform, they maintained active Facebook and Instagram accounts. Plaintiffs accessed the Kaiser Platform from the same device they used to visit

Facebook and Instagram, and Meta associated the data it collected about them from the Kaiser Platform with their Facebook and Instagram accounts.

94. Meta offers an analogous mobile version of the Meta Pixel known as a software development kit (SDK) to app developers. Meta's SDK allows app developers "to track events, such as a person installing your app or completing a purchase." By tracking these events developers can measure ad performance and build audiences for ad targeting.

95. Meta's SDK collects three types of App Events. Automatically Logged Events "logs app installs, app sessions, and in-app purchases." Standard Events are "popular events that Facebook has created for the app." Custom Events are "events [the app developer] create that are specific to [the] app."

96. Once the data intercepted through the Meta Pixel or SDK is processed, Meta makes this data available through its Events Manager, along with tools and analytics to reach these individuals through future Facebook ads. For instance, this data can be used to create "custom audiences" to target the user, as well as other Facebook users who match members' of the audiences' criteria.

97. In addition to using the data intercepted through the Meta Pixel and the SDK to provide analytics services, Meta uses this data to improve its personalized content delivery, advertising network, and machine-learning algorithms, including by improving its ability to identify and target users.

98. Meta has no way to limit or prohibit the use of data collected through the Meta Pixel and its SDK given Meta's open systems and advanced algorithms.

99. According to leaked internal Meta documents, one employee explained "[y]ou pour that ink [i.e., data] into a lake of water . . . and it flows . . . everywhere . . . How do you put that ink back in the bottle? How do you organize it again, such that it only flows to the allowed places in the lake?"

100. In these same leaked documents, another employee explained Meta does "not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X

data for Y purpose.' And yet, that is exactly what regulators expect us to do, increasing our risk of mistakes and misrepresentation." Thus, once the data enters the Meta system, either through its SDK or Pixel, the data can be used for any and all purposes.

101. Meta's own employees confirmed no one at Meta can state confidently where all the data about a user is stored and used. In a recent court hearing as part of the Cambridge Analytica scandal of 2018, Meta's own engineers testified there was not a "single person" at Meta who could answer that question.

102. The Meta Pixel and SDK are incorporated on the Kaiser Platform. As a result, Meta intercepted users' interactions on the Kaiser Platform. For instance, Meta received users' specific responses to medical history and other health questions Kaiser asked in connection with a medical consultation. This included highly sensitive medical information.

103. Plaintiffs provided their PII, health information, and other sensitive data to Kaiser to obtain medical treatment and/or advice, this information was sent to Meta.

104. Plaintiffs did not consent to the interception of their data by Meta. Meta's interception of Plaintiffs' PII, health data, and other highly sensitive information without their consent is an invasion of privacy and violates several laws, including CIPA.

F. Google's Tracking Technology on the Kaiser Platform

105. Google is one of the largest advertising companies in the country. To date, Google generates nearly 77.8% of its revenue through advertising bringing in a grand total of $305.6 billion.

106. Google's advertising business has been extremely successful due, in large part, to Google's ability to target people at a granular level.

107. Given the highly specific data used to target specific users, it is no surprise that millions of companies and individuals utilize Google's advertising services. Google generates substantially all of its revenue from selling advertisement placements.

108. Google embeds a code on a third-party website that tracks a users' activity as the users navigate through a website. As soon as a user takes any action on a webpage that includes this code, the code embedded in the page re-directs the content of the user's communication to Google while the exchange of the communication between the user and website provider is still occurring.

109. Through this technology, Google intercepts each page a user visits, what buttons they click, as well as specific information they input into the website and what they searched. The code sends each of these pieces of information to Google with other identifiable information, such as the users IP address. Google stores this data on its own server, in some instances, for years on end.

110. This data is often associated with the individual users' Google account. For example, if the user is logged into their Google account when the user visits Kaiser's website, Google receives third party cookies allowing Google to link the data collected by the code to the specific Google user.

111. Importantly, even if the code collects data about a non-Google user, Google still retains and uses the data collected through the code in its analytics and advertising services. These non-users are referred to as having "shadow profiles" with Google.

112. At the time Plaintiffs used the Kaiser Platform, they maintained active Google accounts. Plaintiffs accessed the Kaiser Platform from the same device they used to visit Google, and Google associated the data it collected about them from the Kaiser Platform with their Google accounts.

113. Google's codes are incorporated on the Kaiser Platform. As a result, Google intercepted users' interactions on the Kaiser Platform. For instance, Google received users' specific responses to medical history and other health questions Kaiser asked in connection with a medical consultation. This included highly sensitive medical information.

114. Plaintiffs provided their PII, health information, and other sensitive data to Kaiser to obtain medical treatment and/or advice, this information was sent to Google.

115. Plaintiffs did not consent to the interception of their data by Google. Google's interception of Plaintiffs' PII, health data, and other highly sensitive information without their consent is an invasion of privacy and violates several laws, including CIPA.

G. Plaintiffs and the Class Members do not consent to Google and Meta's Conduct

116. Plaintiffs and Class members had no way of knowing that Google and Meta were intercepting their communications when interacting with the Kaiser Platform because their software is inconspicuously incorporated in the background.

117. This conduct is all the more egregious given the nature of the information entered into the Kaiser Platform, e.g., PII, requests for prescriptions, and identifiable medical information, among other things. Plaintiffs and Class members would not expect this information to be intercepted without their consent.

118. This is especially true given Kaiser's consistent representations that this information would remain private and confidential as discussed above. Kaiser repeats these assurances throughout its privacy policy. Accordingly, users' "data is held to even stricter privacy standard than required by CCPA (Health Insurance Portability and Accountability Act ("HIPAA") and California Confidentiality of Medical Information Act, as some examples.)"

119. Accordingly, Plaintiffs and Class members did not consent to Defendants' conduct.

H. Plaintiffs and the Class have a Reasonable Expectation of Privacy in their User Data

120. Plaintiffs and Class members have a reasonable expectation of privacy in their communications on the Kaiser Platform, including their health information.

121. Privacy polls and studies uniformly show that the overwhelming 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' personal data.

122. For example, a recent 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 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. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.

123. Users act consistent with these preferences. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.

124. Another recent study by DataGrail revealed that 67% of people were willing to pay $100 or more annually to keep their information out of the hands of companies and the government.

The same study revealed that 75% of people would abandon brands that do not take care of their data.

125. Other privacy law experts have expressed concerns about the disclosure to third parties of a users' intimate health data. For example, Dena Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra Labs—explained that having your personal health information disseminated in ways you are unaware of could have serious repercussions, including affecting your ability to obtain life insurance and how much you pay for that coverage, increase the rate you're charged on loans, and leave you vulnerable to workplace discrimination.

126. This data is also extremely valuable. According to Experian, health data is a "gold mine" for healthcare companies and clinicians.

127. Consumers' health data, including what prescriptions they have, are extremely profitable. For instance, Datarade.ai advertises access to U.S. customers names, addresses, email addresses, telephone numbers who bought brand name medicine. The starting price for access to just some of this data was $10,000. Other companies, like Pfizer, spend $12 million annually to purchase health data and the medical data industry itself was valued at over $2.6 billion back in 2014.

128. Defendants' surreptitious interception of Plaintiffs' and Class members' private communications, including PII, health information, and other sensitive data violates Plaintiffs' and Class members' privacy interests.

V.

TOLLING, CONCEALMENT, AND ESTOPPEL

129. The applicable statutes of limitation have been tolled as a result of Defendants' knowing and active concealment and denial of the facts alleged herein.

130. Meta and Google's software was secretly incorporated into the Kaiser Platform, providing no indication to users that they were interacting with sites that shared their data, including PII and medical information, with third parties.

131. Google and Meta had exclusive knowledge that the Kaiser Platform incorporated its software, yet failed to disclose that fact to users, or that by interacting with the Kaiser Platform, Plaintiffs' and Class members' sensitive data, including PII and health data, would be intercepted by third parties.

132. Plaintiffs were, at all times, diligent in using the Kaiser Platform. Nevertheless, Plaintiffs and Class members could not with due diligence have discovered the full scope of Google and Meta's conduct, including because it is highly technical and there were no disclosures or other indication that would inform a reasonable consumer that third parties, including Google and Meta, were intercepting, data from the Kaiser Platform.

133. The earliest Plaintiffs and Class members could have known about Google and Meta's conduct was shortly before the filing of this Complaint through the investigation of counsel.

134. Google and Meta were under a duty to disclose the nature and significance of their data collection practices but did not do so. Google and Meta are therefore estopped from relying on any statute of limitations under the discovery rule.

135. Additionally, Google and Meta engaged in fraudulent conduct to prevent Plaintiffs and Class members from discovering the interception of their data. Kaiser misled Plaintiffs and Class members to believe their data, including health information and PII, would not be intercepted.

136. Kaiser represented to Plaintiffs and Class members that they applied even stronger restrictions on the sharing of data than those imposed by HIPAA and the CMIA. It also promised Plaintiffs and Class members that their "personal information" would not be shared. No Defendant disclosed the misconduct alleged herein.

137. Meta concealed in its Privacy Policy that it collects PII and medical information from Kaiser Platform users, as well as any form of medical information from any source. Meta maintains a Privacy Policy through which it purports to help users "understand what information we collect, and how we use and share it." Meta claims it is "important to [Meta] that [users] know how to control [their] privacy."[13]

[13] Privacy Policy, META PLATFORMS, INC. (effective December 27, 2023), https://www.facebook.com/privacy/policy/ last visited on June 8, 2024.

138. This was false. Meta does not disclose, in this purportedly comprehensive policy, that it will collect medical information and PII from Kaiser users. Quite the opposite, Meta represents in its Privacy Policy it only collects "information when you visit [a] site or app" when its "partners . . . have the right to collect, use and share your information before giving it to us." *Id.* This, combined with Kaiser's own representations, would lead Kaiser users to believe their medical information and PII was not collected or used by Meta because Kaiser promised and disavowed that it would share this type of information.

139. Google too concealed its own data interception practices. Like Meta, Google maintains a Privacy Policy that states "When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control," such that it provides a policy that "is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.."[14] The only sentence in this long policy that could remotely apply to the collection of Kaiser users' data states "Google works with businesses and organizations in a variety of ways. We refer to these businesses and organizations as "partners". For example, over 2 million non-Google websites and apps partner with Google to show ads." Google could disclose, but concealed, who these "partners" were and that the vague similar information it referenced that it may collect included highly sensitive medical information and PII. Google did not, choosing to conceal this information to continue collecting it undetected. *Id.*

140. Plaintiffs and Class members were not aware that Google and Meta intercepted their data, including PII and health information.

141. Plaintiffs and Class members exercised due diligence to uncover the facts alleged herein and did not have actual or constructive knowledge of Defendants' misconduct by virtue of their fraudulent concealment.

142. Accordingly, all statutes of limitations are tolled under the doctrine of fraudulent concealment.

[14] Privacy Policy, Google (effective March 28, 2024), https://policies.google.com/privacy?hl=en-US last visited on June 8, 2024.

VI.

CLASS ACTION ALLEGATIONS

143. Class Representative Plaintiffs bring this action on their own behalf and on behalf of all other persons similarly situated. The putative class that Class Representative Plaintiffs seek to represent is composed of: "All natural persons in the United States who used the Kaiser Platform and whose communications and/or data were intercepted by Defendants, and who received a Notice of Data Breach in May of 2024." Excluded from the Class are the natural persons who are directors, and officers, of the Defendants, as well as Plaintiffs' counsel, judges, clerks, and other supporting staff of the Superior Court of California by and for the County of Alameda. Class Representative Plaintiffs expressly disclaims that he is seeking a class-wide recovery for personal injuries attributable to Defendant's conduct.

144. Plaintiffs are informed and believe that the members of the Class are so numerous that joinder of all members is impracticable. While the exact number of the Class members is unknown to Class Representative Plaintiffs at this time, such information can be ascertained through appropriate discovery, from records maintained by Defendants. According to Kaiser's filings with the United States Department of Health and Human Services, 13.4 million consumers, including 9.6 million Californians, were affected by this intentional sale of confidential medical information.

145. There is a well-defined community of interest among the members of the Class because common questions of law and fact predominate, Class Representative Plaintiffs' claims are typical of the members of the class, and Class Representative Plaintiffs can fairly and adequately represent the interests of the Class.

146. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class are:

(a) Whether Defendants failed to adequately safeguard Plaintiffs and the Class's Personal and Medical Information;

(b) Whether Defendants sold information to third party advertisers;

(c) Whether the type of information sold by Defendants to third party advertisers constitutes confidential medical information as defined by Civil Code §56.05(j);

(d) Whether Defendants failed to protect Plaintiffs and the Class's Personal and Medical Information;

(e) Whether Defendants' policy of selling data gathered from the Class on its websites and web applications violated the FTC Act, HIPAA, CMIA, and/or Defendants' other duties;

(d) Whether Defendants violated the data security statutes and notification statutes applicable to Plaintiffs and the Class;

(e) Whether Defendants failed to notify Plaintiffs and members of the Class about the unauthorized release expeditiously and without unreasonable delay after the unauthorized release was discovered;

(f) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Class Members' Personal and Medical Information properly and as promised;

(g) Whether Defendants entered into implied contracts with Plaintiffs and the members of the Class that included contract terms requiring Defendants to protect the confidentiality of Personal and Medical Information and have reasonable security measures;

(h) Whether Defendants violated the consumer protection statutes and state medical privacy statutes applicable to Plaintiffs and the Class;

(i) Whether Defendants failed to notify Plaintiffs and Class Members about the unauthorized release as soon as practical and without delay after the unauthorized release was discovered;

(j) Whether Defendants' conduct described herein constitutes a breach of their implied contracts with Plaintiffs and the Class;

(k) Whether Plaintiffs and the members of the Class are entitled to damages as a result of Defendants' wrongful conduct;

(l) What equitable relief is appropriate to redress Defendants' wrongful conduct;

(m) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Plaintiffs and members of the Class;

(n) Whether Defendants acted negligently in failing to safeguard Plaintiffs' and the Class's Personal and Medical Information, including whether its conduct constitutes negligence;

(o) Whether Defendants acted negligently in failing to safeguard Plaintiffs' and the Class's Personal and Medical Information, including whether its conduct constitutes negligence *per se*;

(p) Whether Defendants violated Plaintiffs' and Class members' privacy rights;

(q) Whether Defendants' acts and practices violated the Common Law Invasion of Privacy;

(r) Whether Defendants were unjustly enriched;

(s) Whether Defendants' acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, et seq;

(t) Whether Plaintiffs and the Class members are entitled to equitable relief, including, but not limited to, injunctive relief, restitution, and disgorgement; and

(u) Whether Plaintiffs and the Class members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

Class Representative Plaintiffs' claims are typical of those of the other Class members because Class Representative Plaintiffs, like every other Class member, were exposed to virtually identical conduct and is entitled to nominal damages of one thousand dollars ($1,000) per violation pursuant to Civil Code §§ 56.101 and 56.36(b)(1).

147. Class Representative Plaintiffs will fairly and adequately protect the interests of the Class. Moreover, Class Representative Plaintiffs have no interest that is contrary to or in conflict with those of the Class they seek to represent during the Class Period. In addition, Class Representative Plaintiffs have retained competent counsel experienced in class action litigation to further ensure such protection and intend to prosecute this action vigorously.

148. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for the Defendant in the State of California and would lead to repetitious trials of the numerous common questions of fact and law in the State of California. Class Representative Plaintiffs know of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action. As a result, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

149. Proper and sufficient notice of this action may be provided to the Class members through direct mail.

150. Moreover, the Class members' individual damages are insufficient to justify the cost of litigation, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Absent certification of this action as a class action, Class Representative Plaintiffs and the members of the Class will continue to be damaged by the unauthorized release of their individual identifiable medical information.

//

VII.

CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS

151. California substantive laws apply to every member of the Class. California's substantive laws may be constitutionally applied to the claims of Plaintiffs and the Classes under the Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by Plaintiffs and Class members, thereby creating state interests to ensure that the choice of California state law is not arbitrary or unfair.

152. Meta and Google maintain their principal places of business in California and conduct substantial business in California, such that California has an interest in regulating Meta and Google's conduct under its laws. Meta also selected California law as the law to govern all disputes with their customers in their respective terms of service. Defendants Meta and Google's decision to reside in California and avail themselves of California's laws renders the application of California law to the claims herein constitutionally permissible.

153. The application of California laws to the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiffs and the proposed Class, and California has a greater interest in applying its laws here given Defendants' locations and the location of the conduct at issue than any other interested state.

VIII.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
(Violations of the Confidentiality of Medical Information Act, Civil Code § 56, *et seq.*)
(Against All Defendants)

154. Plaintiffs and the Class incorporate by reference all of the above paragraphs of this Complaint as though fully stated herein.

155. Kaiser is a "provider of health care," within the meaning of Civil Code § 56.05(m), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), of "patients" of the Kaiser, within the meaning of Civil Code § 56.05(k).

156. Plaintiffs and the Class are "patients" of Kaiser within the meaning of Civil Code § 56.05(k). Furthermore, Plaintiffs and the Class, as patients of Kaiser, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), stored onto Kaiser's server, and received treatment at one of Kaiser's hospital, satellite, or urgent care locations on or before October 2023. Plaintiffs and the Class also utilized Kaiser's website and/or web application to research medical conditions, make appointments with their physicians for specific medical conditions, email their physicians regarding medical questions they had, amongst other medical uses.

157. On April 26, 2027, Plaintiffs and the Class were informed through an article on Techcrunch, along with other media outlets that Kaiser released to "third-party advertisers, including Google, Microsoft and X (formerly Twitter)" Plaintiffs' and the Class's individual identifiable "medical information," within the meaning of Civil Code § 56.05(j),[15] including "member names and IP addresses, as well as information that could indicate if members were signed into a Kaiser Permanente account or service and how members "interacted with and navigated through the website and mobile applications, and search terms used in the health encyclopedia." [16]

158. A similar Email Notice was sent by Kaiser to Plaintiffs and the Class on or about May 13, 2024.

159. Despite realizing the unauthorized release of Plaintiffs' personal medical information, Kaiser belatedly informed Plaintiffs and the Class Members about the approximate duration of the issue in its policies and procedures that allowed unauthorized individual(s) access to Plaintiffs' and the Class Members' personal medical information.

[15] Pursuant to Civil Code § 56.05(j), "Medical information" means "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 elements of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity."

[16] Whittaker, Zack. "Health insurance giant Kaiser will notify millions of a data breach after sharing patients' data with advertisers," https://techcrunch.com/2024/04/25/kaiser-permanente-health-plan-millions-data-breach/ last accessed on April 26, 2024.

160. As a result of Kaiser's above-described conduct, Plaintiffs and the Class have suffered damages from the unauthorized release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10 and 56.101.

161. Because Civil Code § 56.101 allows for the remedies and penalties provided under Civil Code § 56.36(b), Plaintiffs individually and on behalf of the Class seek nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1); and Plaintiffs individually seek actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2).

SECOND CAUSE OF ACTION
(Violations of the CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §17200, *et seq.*)
(Against All Defendants)

162. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

163. Defendant Kaiser is organized under the laws of California, while Defendants Meta and Google have principal offices and do business in California. Defendants violated California's Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard their Personal and Medical Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that they did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the Class's Personal and Medical Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's Personal and Medical Information;

b. by soliciting and collecting Class members' Personal and Medical Information with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Class members' Personal and Medical Information in an unsecure environment;

c. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq.*;

d. by violating the CIPA; and

e. by violating the CMIA, Cal. Civ. Code § 56, *et seq.*

164. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Class members. Defendants' practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the CIPA, FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq.*, and the CMIA, Cal. Civ. Code § 56, *et seq.*

165. As a direct and proximate result of Defendants' unfair and unlawful practices and acts, Plaintiffs and the Class were injured and lost money or property, including but not limited to the overpayments Defendants received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their Personal and Medical Information, and additional losses described above. In addition, Defendants treated the personal and medical information of Plaintiffs and the Class as their own property, and sold it for profit, causing a loss of money and property to Plaintiffs and the Class.

166. Defendants knew or should have known that its sale of information to third party advertisers would violate the CIPA, CMIA, HIPAA and the FTC, and would fail to safeguard Plaintiffs and Class members' Personal and Medical Information. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were intentional, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

167. The conduct and practices described above emanated from California where decisions related to Defendants' advertising and data security were made.

168. Plaintiffs seek relief under the UCL, including restitution to the Class of money or property that the Defendants may have acquired, including all monies it received through the sale of this medical information, by means of Defendants' deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

THIRD CAUSE OF ACTION
(NEGLIGENCE)
(Against Defendant Kaiser)

169. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

170. Kaiser required Plaintiffs and Class Members to submit non-public, sensitive PII and other data via its contracts with the respective health care providers.

171. Kaiser had, and continues to have, a duty to Plaintiffs and Class Members to exercise reasonable care in safeguarding and protecting their Private Information and other data. Kaiser also had, and continues to have, a duty to use ordinary care in activities from which harm might be reasonably anticipated, such as in the collection, storage and protection of Private Information and other data within their possession, custody and control and that of its vendors.

172. Kaiser's duty to use reasonable security measures arose as a result of the special relationship that existed between Kaiser and patients and former patients. The special relationship arose because Plaintiffs and the Members of the Class had entrusted Kaiser with their Private Information and other data by virtue of being patients at the respective health care providers with which Kaiser had contracted to provide services. Only Kaiser was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and the Class Members from a data breach.

173. Kaiser violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs and Class Members' Private Information and other data by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the Private Information and other data entrusted to it,

including Plaintiffs' and Class Members' Private Information and other data as aforesaid. It was reasonably foreseeable to Kaiser that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information and other data by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' Private Information and other data.

174. Kaiser, by and through its negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiffs and Class Members by, inter alia, failing to exercise reasonable care in safeguarding and protecting Plaintiffs and Class Members' Private Information and other data within their possession, custody and control.

175. Kaiser, by and through its negligent actions, inactions, omissions, and want of ordinary care, further breached its duties to Plaintiffs and Class Members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their Private Information and other data.

176. But for Kaiser's negligent breach of the above-described duties owed to Plaintiffs and Class Members, their Private Information and other data would not have been released, disclosed, and disseminated without their authorization.

177. Plaintiffs' and Class Members' Private Information and other data was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Kaiser's failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class Members' Private Information and other data.

178. As a direct and proximate result of Kaiser's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class Members have suffered, and will continue to suffer, ongoing, imminent,

and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and noneconomic harm.

179. Kaiser's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this Data Breach constitute negligence.

180. Plaintiffs are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

181. Plaintiffs are also entitled to injunctive relief requiring Kaiser to, e.g., (i) strengthen its data security programs and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide robust and adequate credit monitoring to all Class Members, and any other relief this Court deems just and proper.

FOURTH CAUSE OF ACTION
(NEGLIGENCE PER SE)
(Against Defendant Kaiser)

182. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

183. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Kaiser had a duty to provide fair and adequate computer systems and data security to safeguard the personal and financial information of Plaintiffs and Class Members.

184. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Kaiser, of failing to use reasonable measures to protect the Private Information and other data of Plaintiffs and Class Members. The pertinent FTC publications and orders form part of the basis of Kaiser's duty in this regard.

185. Kaiser required, gathered, and stored personal and financial information of Plaintiffs and Class Members to fulfill its contracts with the various and several health care providers.

186. Kaiser violated the FTCA by failing to use reasonable measures to protect the Private Information and other data of Plaintiffs and Class Members and by not complying with applicable industry standards, as described herein.

187. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

188. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

189. As a direct and proximate result of Kaiser's negligence per se, Plaintiffs and Class Members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their needing to contact agencies administering unemployment benefits; potentially defending themselves from legal action base upon fraudulent applications for unemployment benefits made in their name; contacting their financial institutions; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

190. Kaiser's violation of the FTCA constitutes negligence per se.

191. For the same reasons and upon the same bases, Kaiser's violation of the CMIA, UCL, and various other State and local statutes, constitutes negligence per se.

192. As a direct and proximate result of Kaiser's violation of the foregoing statutes and regulations, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
Violation of Common Law Invasion of Privacy – Intrusion Upon Seclusion
(Against Defendants Google and Meta)

193. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

194. Plaintiffs asserting claims for intrusion upon seclusion must plead (1) that the defendant intentionally intruded into a place, conversation, or matter as to which Plaintiffs have a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

195. Google and Meta's surreptitious interception, storage, and use of Plaintiffs' and Class members' interactions and communications with the Kaiser Platform, including PII, health information, and prescription requests, constitutes an intentional intrusion upon Plaintiffs' and Class members' solitude or seclusion.

196. Plaintiffs and Class members expected this information to remain private and confidential given the nature of the Kaiser Platform, which is primarily used to receive medical advice, treatment, and prescriptions.

197. This expectation is especially heightened given Kaiser's consistent representations that this data would remain confidential. Plaintiffs and Class members did not expect third parties, and specifically Google and Meta, to secretly intercept this information and their communications.

198. Plaintiffs and Class members did not consent to, authorize, or know about Google and Meta's intrusion at time it occurred. Plaintiffs and Class members never agreed that Google and Meta could intercept, store, and use this data.

199. Google and Meta's intentional intrusion on Plaintiffs' and Class members' solitude or seclusion would be highly offensive to a reasonable person. Plaintiffs and Class members reasonably expected, based on Kaiser's repeated assurances, that their information would not be collected by Google and Meta.

200. The surreptitious taking and interception of sensitive data, including PII and medical information, from millions of individuals was highly offensive because it violated

expectations of privacy that have been established by social norms. Privacy polls and studies show that the overwhelming majority of Americans believe one of the most important privacy rights is the need for an individual's affirmative consent before personal data is collected or shared.

201. The offensiveness of this conduct is all the more apparent because Google and Meta's interception, storage, and use of this information was conducted inconspicuously in a manner that Plaintiffs and Class members would be unable to detect and was contrary to the actual representations made by Kaiser.

202. Given the highly sensitive nature of the data that Google and Meta intercepted, such as private details about medications and health information, this kind of intrusion would be (and in fact is) highly offensive to a reasonable person.

203. As a result of Google and Meta's actions, Plaintiffs and Class members have suffered harm and injury, including, but not limited to, an invasion of their privacy rights.

204. Plaintiffs and Class members have been damaged as a direct and proximate result of Google and Meta's invasion of their privacy and are entitled to just compensation, including monetary damages.

205. Plaintiffs and Class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class members for the harm to their privacy interests as well as a disgorgement of profits made by Google and Meta as a result of its intrusions upon Plaintiffs' and Class members' privacy.

206. Plaintiffs and Class members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Google and Meta's actions, directed at injuring Plaintiffs and Class members in conscious disregard of their rights. Such damages are needed to deter Google and Meta from engaging in such conduct in the future.

207. Plaintiffs also seek such other relief as the Court may deem just and proper.

SIXTH CAUSE OF ACTION
Violation of CIPA, Cal. Penal Code § 631
(Against Defendants Google and Meta)

208. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

209. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, et seq. ("CIPA") finding 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." *Id.* § 630. Thus, the intent behind CIPA is "to protect the right of privacy of the people of this state." *Id*.

210. Cal. Penal Code § 631 imposes liability on any person who "by means of any machine, instrument, contrivance, or in any other manner" (1) "intentionally taps, or makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument," (2) "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 [the state of California]," (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained," or (4) "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."

211. Defendants Google and Meta are persons for purposes of § 631.

212. Defendants Meta and Google maintain their principal places of business in California, where they designed, contrived, agreed, conspired, effectuated, and/or received the interception and use of the contents of Plaintiffs' and Class members' communications. Additionally, Meta has adopted California substantive law to govern their relationship with users.

213. Meta and Google's software, Plaintiffs' and Class members' browsers and mobile applications, and Plaintiffs' and Class members' computing and mobile devices are a "machine, instrument, contrivance, or . . . other manner."

214. At all relevant times, Meta, and Google, using their software, intentionally tapped or made unauthorized connections with, the lines of internet communication between

Plaintiffs and Class members and the Kaiser Platform without the consent of all parties to the communication.

215. Meta and Google willfully and without the consent of Plaintiffs and Class members, reads or attempt to reads, or learn the contents or meaning of Plaintiffs' and Class members' communications to Kaiser while the communications are in transit or passing over any wire, line or cable, or were being received at any place within California when it intercepted Plaintiffs' and Class members' communications and data with Kaiser, who is headquartered in California, in real time.

216. Google and Meta used or attempted to use the communications and information they received through their technology, including to supply analytics and advertising services.

217. The interception of Plaintiffs' and Class members' communications was without authorization and consent from the Plaintiffs and Class members. Accordingly, the interception was unlawful and tortious.

218. Plaintiffs and the Class members seek statutory damages in accordance with § 637.2(a), which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiffs and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

219. Plaintiffs and Class members have also suffered irreparable injury from these unauthorized acts. Plaintiffs' and Class members' sensitive data has been collected, viewed, accessed, and stored by Google and Meta, has not been destroyed, and due to the continuing threat of such injury, Plaintiffs and Class members have no adequate remedy at law, Plaintiffs and Class members are entitled to injunctive relief.

SEVENTH CAUSE OF ACTION
Violation of CIPA, Cal. Penal Code § 632
(Against Defendants Google and Meta)

220. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

221. Cal. Penal Code § 632 prohibits "intentionally and without the consent of all parties to a confidential communication," the "use[] [of] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication[.]"

222. Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

223. Plaintiffs' and Class members' communications to Kaiser, including their sensitive medical information including information concerning medications they were taking or were prescribed, their medical histories, allergies, and answers to other health-related questions, were confidential communications for purposes of § 632, including because Plaintiffs and Class members had an objectively reasonable expectation of privacy in this data.

224. Plaintiffs and Class members expected their communications to Kaiser to be confined to Kaiser, in part because of Kaiser's consistent representations that these communications would remain confidential. Plaintiffs and Class members did not expect third parties, and specifically Google and Meta, to secretly eavesdrop upon or record this information and their communications.

225. Google and Meta's software are all electronic amplifying or recording devices for purposes of § 632.

226. By contemporaneously intercepting and recording Plaintiffs' and Class members' confidential communications to Kaiser through the Google and Meta's software, Google and Meta eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

227. At no time did Plaintiffs or Class members consent to Defendants' conduct, nor could they reasonably expect that their communications to Kaiser would be overheard or recorded by Google and Meta.

228. Kaiser and Meta utilized Plaintiffs' and Class members' sensitive medical information for their own purposes, including advertising and analytics.

229. Plaintiffs and Class members seek statutory damages in accordance with § 637.2(a) which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiffs and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

230. Plaintiffs and Class members have also suffered irreparable injury from these unauthorized acts. Plaintiffs' and Class members' sensitive data has been collected, viewed, accessed, and stored by Google and Meta, has not been destroyed, and due to the continuing threat of such injury, Plaintiffs and Class members have no adequate remedy at law, Plaintiffs and Class members are entitled to injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request the Court to grant Plaintiffs and the Class members the following relief against Defendants:

a. An order certifying this action as a class action under Code of Civil Procedure §382, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual and statutory damages, including statutory damages under the CIPA, CMIA, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein, including, but not limited to:

i. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

ii. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

iv. Ordering that Defendants' segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

v. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

vi. Ordering that Defendants conduct regular database scanning and securing checks;

vii. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain an unauthorized release when it occurs and what to do in response to an unauthorized release; and

viii. Ordering Defendants to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.;

d. An order requiring Defendants to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. Restitutionary disgorgement of all wrongly acquired monies received by Defendants from the sale of the medical information of Plaintiffs and the Class Members, including monies directly received from advertisers;

f. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law, including the UCL, Cal. Bus. & Prof. Code § 17082 and the CMIA, Cal. Civ. Code 56.35; and

g. An award of such other and further relief as this Court may deem just and proper.

POTTER HANDY LLP

Dated: June 10, 2024 By: /s/ James M. Treglio
Mark D. Potter, Esq.
James M. Treglio, Esq.
Attorneys for the Plaintiffs and the Class

DEMAND FOR JURY TRIAL

Plaintiffs and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

POTTER HANDY LLP

Dated: June 9, 2024 By: /s/ James M. Treglio
Mark D. Potter, Esq.
James M. Treglio, Esq.
Attorneys for the Plaintiffs and the Class