KESSLER TOPAZ
MELTZER & CHECK, LLP
Jennifer L. Joost (Bar No. 296164)
jjoost@ktmc.com
One Sansome Street, Suite 1850
San Francisco, CA 94104
Telephone: (415) 400-3000
Facsimile: (415) 400-3001

-and-

KESSLER TOPAZ
MELTZER & CHECK, LLP
Joseph H. Meltzer (appearance *pro hac vice*)
jmeltzer@ktmc.com
Melissa L. Yeates (appearance *pro hac vice*)
myeates@ktmc.com
Tyler S. Graden (appearance *pro hac vice*)
tgraden@ktmc.com
Jordan E. Jacobson (Bar No. 302543)
jjacobson@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056

CARELLA BYRNE CECCHI
BRODY & AGNELLO, P.C.
James E. Cecchi (appearance *pro hac vice*)
jcecchi@carellabyrne.com
Michael A. Innes (*pro hac vice* forthcoming)
minnes@carellabyrne.com
Kevin G. Cooper (appearance *pro hac vice*)
kcooper@carellabyrne.com
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700
Facsimile: (973) 994-1744

Interim Class Counsel
(*Additional Attorneys Listed on Signature Page*)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JOHN DOE, JOHN DOE II, JOHN DOE III, JANE DOE, JANE DOE II, JANE DOE III, JANE DOE IV, JANE DOE V, and ALEXIS SUTTER, Individually and on behalf of all others similarly situated,

Plaintiffs,

v.

KAISER FOUNDATION HEALTH PLAN, INC., KAISER FOUNDATION HOSPITALS, and KAISER FOUNDATION HEALTH PLAN OF WASHINGTON,

Defendants.

Case No. 3:23-cv-02865-EMC

CONSOLIDATED MASTER CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

REDACTED

TABLE OF CONTENTS

Plaintiffs John Doe, John Doe II, John Doe III, Jane Doe, Jane Doe II, Jane Doe III, Jane Doe IV, and Jane Doe V,[1] and Alexis Sutter, (collectively, "Plaintiffs") bring this proposed class action against Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and the Kaiser Foundation Health Plan of Washington (collectively "Kaiser" or "Defendants"), individually and on behalf of all others similarly situated, upon personal knowledge as to Plaintiffs' own conduct, and on information and belief as to all other matters based on investigation by counsel.[2]

I. NATURE OF THE ACTION

1. As any reasonable patient would expect, Plaintiffs trusted that their healthcare providers would treat the information that they shared with them as private and confidential.

2. This expectation extends to Plaintiffs' use of Kaiser's websites and mobile applications, on which they and other Kaiser Plan Members schedule appointments, access medical test results, learn about treatment options, order and review prescriptions, exchange messages and healthcare information with providers, participate in online health assessments, make payments for healthcare, obtain insurance information, and research specialists, among other sensitive activities.

3. Notwithstanding Plaintiffs' and other Kaiser Plan Members'[3] reasonable expectation that their interactions and communications through Kaiser's website and mobile applications would not be shared with third parties, Kaiser discloses individually identifiable personal information and the contents of patients' confidential information and communications with a number of third parties, completely unbeknownst to Plaintiffs and other Kaiser Permanente Members while those communications are in transit between Plaintiffs and Class Members on the one hand and Kaiser on the other.

---

[1] Plaintiffs John Doe, John Doe II, John Doe III, Jane Doe, Jane Doe II, Jane Doe III, Jane Doe IV, and Jane Doe V are proceeding anonymously pursuant to this Court's November 17, 2023 Order Permitting Plaintiffs to Proceed Anonymously. ECF No. 91. This Consolidated Master Class Action Complaint consolidates the first-filed action, *Doe v. Kaiser*, with later filed and consolidated cases *Sutter v. Kaiser Foundation Health Plan, Inc.* (Case No. 24-cv-03352) and *Newton v. Kaiser Foundation Health Plan, Inc. et al.* (No. 24-cv-03625). ECF No. 192.

[2] Counsel's investigation includes an analysis of publicly available information and Defendants' limited production to date. Plaintiffs believe that more fulsome discovery will provide further support for the claims alleged herein and reserve the right to seek leave to amend based on future productions.

[3] Defined below.

4. Specifically, unbeknownst to Plaintiffs and other Kaiser Plan Members, Kaiser has installed code from multiple third parties throughout the Kaiser website[4] and mobile applications[5] that allows third party companies, including but not limited to Quantum Metric, Twitter[6], Adobe, Microsoft Bing, and Google[7] (collectively, "Third Party Wiretappers") to intercept the content of Plaintiffs and Class Members' patient status, identifying information, medical topics researched, choices made, information shared and communications with their medical providers, including personally identifiable medical information, Protected Health Information ("PHI") that Kaiser was required to protect under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d-6, and other confidential information and communications, when that information is in transit.

5. The third party code that Kaiser has installed on the Site and Apps transmits and redirects the content of Plaintiffs and other Class Members' communications, along with their IP addresses and other unique identifiers, to these Third Party Wiretappers from the very moment that a user first loads Kaiser's Site or opens its Apps, and continues as the user navigates through the website, researching and sharing sensitive information.

6. Once the Site loads or the Apps are launched, the Third Party Wiretappers continue to intercept the content of patients' communications with Kaiser in real time as users of the Site or Apps ("Users") access specific medical information, click buttons that divulge sensitive and protected patient status, and personal and health information, and enter information into various fields on Kaiser's Site or Apps, such as: (1) signing-up for a patient Portal; (2) signing-in or signing-out of a

[4] Kaiser operates a website ("Site"), with a homepage located at https://healthy.kaiserpermanente.org/front-door ("Homepage").

[5] Kaiser Plan Members in California, Colorado, the District of Columbia, Georgia, Hawaii, Maryland, Oregon, Virginia, and Southwest Washington can use the "Kaiser Permanente App," and Kaiser Plan Members in Washington outside of Southwest Washington can use the "Kaiser Permanente Washington App," collectively referred to as the "Apps."

[6] Twitter began rebranding itself as X.com in late July 2023. *See* Ryan Mac & Tiffany Hsu, *From Twitter to X: Elon Musk Begins Erasing an Iconic Internet Brand*, N.Y. Times (Jul. 24, 2023), https://www.nytimes.com/2023/07/24/technology/twitter-x-elon-musk.html. As of the time of this Complaint, the change was ongoing.

[7] For the reasons set forth below, the term "Third Party Wiretappers" also includes Dynatrace, LLC ("Dynatrace") with respect to the Kaiser Permanente Washington App and certain portions of the Site that concern Kaiser Permanente operations in or around Washington ("Washington Site").

patient Portal; (3) taking actions inside a patient Portal; (4) making, scheduling, or participating in appointments; (5) reviewing and ordering prescriptions; (6) exchanging communications relating to doctors, treatments, payment information, health insurance information, prescription drugs, prescriptions, side effects, conditions, diagnoses, prognoses, or symptoms of health conditions; and (7) providing other information that qualifies as PHI, "personal health information," and/or identifying information under federal and state laws.

7. Kaiser knew that by embedding the Third Party Wiretappers' code, they were disclosing and permitting these Third Party Wiretappers to intercept and collect information shared by its Users, including the content of Plaintiffs and Class Members' communications, which include identifying information, personal and sensitive information relating to medical treatment and/or PHI that Kaiser was required to protect under HIPAA, its Privacy Statement and the Terms and Conditions of the Site and Apps, and state laws.

8. Despite this knowledge, Kaiser embedded the code on its Site and Apps and on April 12, 2024, one day after this Court issued an opinion on Kaiser's Motion to Dismiss Plaintiffs' First Amended Complaint, Kaiser Foundation Health Plan, Inc., for the first time reported to state and federal agencies [redacted]

Ex. 1.

9. In its recent disclosures, Kaiser further acknowledged that the information disclosed to the Third Party Wiretappers included:

[redacted]

Id. Kaiser further acknowledged that [redacted] *Id.*

10. Kaiser further represented that it was still working to determine: [redacted] *Id.*

11. These disclosures were made by Kaiser on April 12, 2024 to at least the following: the United States Department of Health and Human Services, The Office of the Washington Attorney General, the State of California Department of Justice, [redacted]

12. [redacted]

13. While these disclosures were just recently made, despite Kaiser's knowledge of obligations to report when Kaiser Plan Members' PHI had been exposed, Kaiser had long known that the code it installed on its Site and Apps was allowing the Third Party Wiretappers to collect PHI in violation of HIPAA and other laws, as well as in violation of the Site and Apps' Terms and Conditions and Privacy Statement.

14. Indeed, while Kaiser in its April 12, 2024 disclosures to regulators stated it confirmed on October 25, 2023 that certain Third Party Wiretappers were receiving PHI in violation of HIPAA, ***Kaiser waited nearly six months*** to notify the regulators of its finding despite the fact that the HIPAA Breach Notification Rule (45 CFR §§ 164.400-414) requires that Kaiser provide notification "without unreasonable delay and in no case later than 60 calendar days after discovery." Data breach notification statutes and medical information disclosure statutes in the states where Kaiser operates further required that Kaiser notify the affected residents, Office of the Attorney General, state consumer protection office, state health commissioner, and/or all consumer reporting agencies without undue delay and in the most expedient time possible,[8] with some states requiring the notification to be made no more than thirty[9] or forty-five days[10] after discovering the breach. Kaiser subsequently began notifying Plaintiffs and other Kaiser Plan Members of this breach on or around May 8, 2024. Kaiser's blatantly tactical delay was unfair and unfortunate—this type of information should have been promptly disclosed, rather than being withheld to limit Kaiser Plan Members' ability to pursue claims and Plaintiffs' ability to use this information to oppose Kaiser's Motion to Dismiss.

15. [redacted]

[8] California Customer Records Act, Cal. Civ. Code § 1798.82 ("disclosure shall be made in the most expedient time possible and without unreasonable delay"); District of Columbia Consumer Security Breach Notification Act, D.C. Code § 28-3852 ("notification shall be made in the most expedient time possible and without unreasonable delay"); Georgia Security Breach of Computerized Information Act, Ga. Code § 10-1-912 ("notice shall be made in the most expedient time possible and without unreasonable delay"); Hawaii Security Breach of Personal Information Act, Haw. Rev. Stat. § 487N-2 ("disclosure notification shall be made without unreasonable delay"); Virginia Breach of Personal Information Notification, Va. Code § 18.2-186.6 (disclosure to be made "to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay"); and Virginia Breach of Medical Information Notification, Va. Code § 32.1-127.1:05 (disclosure to be made "to the Office of the Attorney General, the Commissioner of Health, the subject of the medical information, and any affected resident of the Commonwealth without unreasonable delay").

[9] Colorado Notification of Security Breach, Colo. Rev. Stat. § 6-1-716; Washington Personal Information—Notice of Security Breaches, Wash. Rev. Code § 19.255.010.

[10] Maryland Personal Information Protection Act, Md. Code Ann. Com. Law § 14-3504; Oregon Consumer Information Protection Act, Or. Rev. Stat. § 646A.604.

[redacted] Ex. 2, Ex. 3.

16. Kaiser's delay in reporting these disclosures of PHI and other identifying information to third parties was part of a years' long effort to conceal from the public, including Plaintiffs and other Class members, the nature and extent of the PHI that it was unlawfully providing to Third Party Wiretappers.

17. In fact, Kaiser knew that its conduct violated state data breach notification statutes as well as United States Department of Health and Human Services ("HHS") guidance related to HIPAA, and other state laws.

18. Notably, HHS has issued guidance explaining information collected by tracking technologies, like those recently disclosed by Kaiser, may be considered PHI under HIPAA. As detailed in Plaintiffs' First Amended Complaint, HHS issued a bulletin in December 2022 "to highlight the obligations" of health care providers under the HIPAA Privacy Rule "when using online tracking technologies" such as those used by Kaiser which "collect and analyze information about how internet users are interacting with a regulated entity's website or mobile application."[11] As HHS explained:

> Tracking technologies collect information and track users in various ways, many of which are not apparent to the website or mobile app user. Websites commonly use tracking technologies such as cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts to track and collect information from users. Mobile apps generally include/embed tracking code within the app to enable the app to collect information directly provided by the user, and apps may also capture the user's mobile device-related information. **For example, mobile apps may use a unique identifier from the app user's mobile device, such as a device ID or advertising. These unique identifiers, along with any other information collected by the app, enable the mobile app owner or vendor or any other third party who receives such information to create individual profiles about each app user**.

[11] Press Release, *HHS Office of Civil Rights Issue Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information*, HHS (Dec. 1, 2022), https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html; *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, HHS (Dec. 1, 2022, updated June 26, 2024), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

19. In the bulletin, which HHS amended on March 18, 2024, HHS confirmed that HIPAA applies to health care providers' use of tracking technologies, like those developed by the Third Party Wiretappers and used by Kaiser. Among other things, HHS explained that health care providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information, even if no treatment information is included and even if the individual does not have a relationship with the health care provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> Some Regulated entities may be disclosing a variety of information to tracking technology vendors through tracking technologies placed on the regulated entity's website or mobile app, such as information that the individual types or selects when they use regulated entities' websites or mobile apps. The information disclosed might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, device IDs, or any unique identifying code. In some cases, the information disclosed may meet the definition of individually identifiable health information (IIH), which is a necessary pre-condition for information to meet the definition of PHI when it is transmitted or maintained by a regulated entity.

20. On June 26, 2024, HHS again issued updated guidance in light of the court's order.[12] This guidance continues to maintain that "[t]racking technologies on a regulated entity's user-authenticated webpages," such as Kaiser's Site and Apps, "generally have access to PHI." *Id*. Thus, "a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to only use and disclose PHI in compliance with the HIPAA Privacy Rule." *Id*. Further, the updated guidance noted that while unauthenticated webpages typically "do not have access to individuals' PHI," and thus are "not regulated by the HIPAA Rules," there are circumstances in which "tracking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to the tracking technology vendors." *Id.*

21. This HHS bulletin did not create any new obligations, but instead highlighted obligations that have been in place for decades, with which Kaiser should have been complying.

22. [redacted]

[redacted]

[12] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, HHS (Dec. 1, 2022, updated June 26, 2024), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[redacted]

23. Kaiser's disclosure of Kaiser Plan Members' patient status, identifying information, and personal and sensitive heath information to the Third Party Wiretappers, including without adequate disclosure of its conduct to Plaintiffs and Class Members, constitutes an egregious invasion of Plaintiffs and Class Members' privacy and violates the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; Cal. Const. art. I, § 1; California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56.10, *et seq.*; the Washington Privacy Act, Wash. Rev. Code §§ 9.73, *et seq.*; Washington Health Care Information Act, Wash. Rev. Code §§ 70.02.005, *et seq.*, Washington Consumer Protection Act, §§ 19.86, *et seq.*; District of Columbia Consumer Protection Procedures Act, D.C. Code §§ 28-3901, *et seq.*; District of Columbia Consumer Security Breach Notification Act, D.C. Code §§ 28-3851, *et seq.*; Georgia Computer Systems Protection Act, Georgia Code §§ 16-9-93; Georgia Insurance and Information Privacy Protection Act, Georgia Code §§ 33-39-1, *et seq.*; Maryland Wiretapping and Electronic Surveillance Act, Maryland Code, Courts & Judicial Procedure §§ 10-401, *et seq.*; Maryland Personal Information Protection Act, Md. Code Ann. Com. Law §§ 14-3501, *et seq.*; Maryland Consumer Protection Act, Md. Code Ann. Com. Law §§ 13-101, *et seq.*; Oregon Unlawful Trade Practices Act, Or. Rev. Stat. §§ 646.605, *et seq.*; Oregon Consumer Information Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*; Virginia Computer Crimes Act, Va. Code §§ 18.2-152.1, *et seq.*; Virginia Insurance Information and Privacy Protection Act, Va. Code §§ 38.2-600, *et seq*. and

HIPAA, and constitutes intrusion upon seclusion, negligence, Statutory Larceny Through False Pretenses, Cal. Penal Code §§ 484, 496, and breach of Kaiser's express and implied promises and duties to Users and Kaiser Plan Members, including Plaintiffs and members of the Classes.

II. THE PARTIES

A. Plaintiffs

1. Plaintiff John Doe

24. Plaintiff John Doe is a citizen of California and resides in Victorville, California.[13]

25. Plaintiff John Doe is a Kaiser Foundation Health Plan member and has received medical treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group beginning in or around January 2013.

26. John Doe first obtained medical treatment from Kaiser Foundation Hospitals and/or the Permanente Medical Group under his father's enrollment in Kaiser health plans from approximately January 1, 2013 through March 31, 2021. John Doe also had healthcare coverage under Anthem through John Doe's own employer from April 1, 2019 through April 1, 2021. Beginning on April 1, 2021 and through the present, John Doe was insured by Kaiser through his union.

27. Plaintiff John Doe has regularly used Kaiser's Site, Patient Portal, and Kaiser Permanente App to access medical information and communicate with his health care providers, including making appointments, reviewing and ordering prescriptions, researching providers and medical conditions, communicating with providers, checking medical results, and reviewing his medical history, since approximately January 2014 through the present.

28. Without Plaintiff John Doe's knowledge or consent, Kaiser allowed the Third Party Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or meaning of the contents of his patient status, identifying information, personal and sensitive health information, and confidential communications with his health care providers through Kaiser's website and mobile application while that information and those messages, reports, and/or communications were in

[13] On March 25, 2024, this Court granted Kaiser's Motion to Compel Arbitration of John Doe's claims with leave to amend. *See* ECF No. 82. Plaintiff John Doe's claims are included here to provide additional details regarding his insurance prior to April 1, 2021, and his use of the Site and Kaiser Permanente App prior to April 1, 2021, which this Court found were not pled in the First Amended Complaint.

transit from approximately January 2014 through approximately November 2023 when Kaiser represented to this Court and government regulators that it disabled, deleted, and/or modified the Third Party Wiretappers' code on the Site and Apps.

29. Plaintiff John Doe received a letter from Kaiser Permanente titled "Notice of Data Breach" dated May 31, 2024—nearly a year after this action first began—wherein Kaiser recognized and admitted that it had violated Plaintiff's privacy. The email stated that "[o]n 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." The letter further acknowledged that the information provided to these Third Party Wiretappers included: "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." The letter further stated that, after its investigation into the use of these online technologies, Kaiser Permanente "removed these online technologies from our websites and mobile applications" and also "implemented additional measures with the guidance of experts to safeguard against recurrence of this type of incident."

2. Plaintiff John Doe II

30. Plaintiff John Doe II is a citizen of Georgia and resides in Loganville, Georgia.

31. Plaintiff John Doe II is a Kaiser Foundation Health Plan member and has received medical treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group since in or around January 2023 after purchasing Kaiser insurance in late 2022.

32. Plaintiff John Doe II has regularly used Kaiser's Site, Patient Portal, and Kaiser Permanente App to access medical information and communicate with his health care providers, including making appointments, researching providers and medical conditions, checking medical results, and reviewing his medical history since approximately January 2023.

33. Without Plaintiff John Doe II's knowledge or consent, Kaiser allowed the Third Party Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or meaning of the

contents of his patient status, identifying information, personal and sensitive health information, and confidential communications with his health care providers through Kaiser's website and mobile application while that information and those messages, reports, and/or communications were in transit from approximately January 2023 through approximately November 2023 when Kaiser represented to this Court and government regulators that it disabled, deleted, and/or modified the Third Party Wiretappers' code on the Site and Apps.

34. Plaintiff John Doe II received an email from Kaiser Permanente titled "Notice of Data Breach" dated May 7, 2024 wherein Kaiser recognized and admitted that it had violated Plaintiff's privacy. The email stated that "[o]n 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." The email further acknowledged that the information provided to these Third Party Wiretappers included: "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." The email further stated that, after its investigation into the use of these online technologies, Kaiser Permanente "removed these online technologies from our websites and mobile applications" and also "implemented additional measures with the guidance of experts to safeguard against recurrence of this type of incident."

3. Plaintiff John Doe III

35. Plaintiff John Doe III is a citizen of Colorado and resides in Westminster, Colorado.

36. Plaintiff John Doe III was a Kaiser Foundation Health Plan member from October 2022 to January 2024 and received medical treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group in 2023.

37. Plaintiff John Doe III regularly used Kaiser Permanente's website, Patient Portal, and mobile application since becoming a Kaiser Foundation Health Plan member to access medical information and communicate with his health care providers, including making appointments,

researching providers and medical conditions, checking medical results, and reviewing his medical history.

38. Without Plaintiff John Doe III's knowledge or consent, Kaiser Permanente allowed the Third Party Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or meaning of the contents of his patient status, identifying information, personal and sensitive health information, and confidential communications with his health care providers through Kaiser Permanente's website and mobile application while that information and those messages, reports, and/or communications were in transit.

39. Plaintiff John Doe III received an email from Kaiser Permanente titled "Notice of Data Breach" dated May 6, 2024 wherein Kaiser recognized and admitted that it had violated Plaintiff's privacy. The email stated that "[o]n 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." The email further acknowledged that the information provided to these Third Party Wiretappers included: "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." The email further stated that, after its investigation into the use of these online technologies, Kaiser Permanente "removed these online technologies from our websites and mobile applications" and also "implemented additional measures with the guidance of experts to safeguard against recurrence of this type of incident."

4. Plaintiff Jane Doe

40. Plaintiff Jane Doe is a citizen of Washington, and currently resides in Mukilteo, Washington.

41. Plaintiff Jane Doe is a Kaiser Foundation Health Plan member and has received medical treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group since in or around October 2017.

42. Plaintiff Jane Doe has regularly used Kaiser's Site, Patient Portal, and Kaiser Permanente Washington App, and Washington Site to access medical information and communicate with her health care providers, including making appointments, researching providers and medical conditions, checking medical results, and reviewing her medical history since approximately October 2017.

43. Without Plaintiff Jane Doe's knowledge or consent, Kaiser allowed the Third Party Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or meaning of the contents of her patient status, identifying information, personal and sensitive health information, and confidential communications with her health care providers through Kaiser's website and mobile application while that information and those messages, reports, and/or communications were in transit from approximately October 2017 through approximately November 2023 when Kaiser represented to this Court and government regulators that it disabled, deleted, and/or modified the Third Party Wiretappers' code on the Site and Apps.

44. Plaintiff Jane Doe received an email from Kaiser Permanente titled "Notice of Data Breach" dated May 14, 2024 wherein Kaiser recognized and admitted that it had violated Plaintiff's privacy. The email stated that "[o]n 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." The email further acknowledged that the information provided to these Third Party Wiretappers included: "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." The email further stated that, after its investigation into the use of these online technologies, Kaiser Permanente "removed these online technologies from our websites and mobile applications" and also "implemented additional measures with the guidance of experts to safeguard against recurrence of this type of incident."

5. Plaintiff Jane Doe II

45. Plaintiff Jane Doe II is a citizen of the District of Columbia and resides in Washington, D.C.

46. Plaintiff Jane Doe II is a Kaiser Foundation Health Plan member and has received medical treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group since in or around July 2022.

47. Plaintiff Jane Doe II has regularly used Kaiser's Site, Patient Portal, and Kaiser Permanente App to access medical information and communicate with her health care providers, including making appointments, researching providers and medical conditions, checking medical results, and reviewing her medical history since approximately July 2022.

48. Without Plaintiff Jane Doe II's knowledge or consent, Kaiser allowed the Third Party Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or meaning of the contents of her patient status, identifying information, personal and sensitive health information, and confidential communications with her health care providers through Kaiser's website and mobile application while that information and those messages, reports, and/or communications were in transit from approximately July 2022 through September 30, 2023.

49. Plaintiff Jane Doe II received an email from Kaiser Permanente titled "Notice of Data Breach" dated May 8, 2024 wherein Kaiser recognized and admitted that it had violated Plaintiff's privacy. The email stated that "[o]n 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." The email further acknowledged that the information provided to these Third Party Wiretappers included: "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." The email further stated that, after its investigation into the use of these online technologies, Kaiser Permanente "removed these online technologies from our websites and mobile applications" and also

"implemented additional measures with the guidance of experts to safeguard against recurrence of this type of incident."

6. Plaintiff Jane Doe III

50. Plaintiff Jane Doe III is a citizen of Maryland and resides in West River, Maryland.

51. Plaintiff Jane Doe III is a Kaiser Foundation Health Plan member and has received medical treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group since in or around August 2015.

52. Plaintiff Jane Doe III has regularly used Kaiser's Site, Patient Portal, and Kaiser Permanente App to access medical information and communicate with her health care providers, including making appointments, researching providers and medical conditions, checking medical results, and reviewing her medical history since approximately August 2015.

53. Without Plaintiff Jane Doe III's knowledge or consent, Kaiser allowed the Third Party Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or meaning of the contents of her patient status, identifying information, personal and sensitive health information, and confidential communications with her health care providers through Kaiser's website and mobile application while that information and those messages, reports, and/or communications were in transit from August 2015 through approximately November 2023 when Kaiser represented to this Court and government regulators that it disabled, deleted, and/or modified the Third Party Wiretappers' code on the Site and Apps.

54. Plaintiff Jane Doe III received an email from Kaiser Permanente titled "Notice of Data Breach" dated May 8, 2024 wherein Kaiser recognized and admitted that it had violated Plaintiff's privacy. The email stated that "[o]n 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." The email further acknowledged that the information provided to these Third Party Wiretappers included: "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." The email further stated that, after its investigation into the use of these online technologies, Kaiser Permanente "removed these online technologies from our websites and mobile applications" and also "implemented additional measures with the guidance of experts to safeguard against recurrence of this type of incident."

7. Plaintiff Jane Doe IV

55. Plaintiff Jane Doe IV is a citizen of Virginia and resides in Fairfax, Virginia.

56. Plaintiff Jane Doe IV is a Kaiser Foundation Health Plan member and has received medical treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group since at least July 2006.

57. Plaintiff Jane Doe IV has regularly used Kaiser's Site, Patient Portal, and Kaiser Permanente App to access medical information and communicate with her health care providers, including making appointments, researching providers and medical conditions, checking medical results, and reviewing her medical history since Kaiser made the mobile application available in or around 2012, and has used the Site since approximately July 2006.

58. Without Plaintiff Jane Doe IV's knowledge or consent, Kaiser allowed the Third Party Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or meaning of the contents of her patient status, identifying information, personal and sensitive health information, and confidential communications with her health care providers through Kaiser's website and mobile application while that information and those messages, reports, and/or communications were in transit from approximately July 2006 for the Site, and approximately 2012 for the mobile application, through approximately November 2023 when Kaiser represented to this Court and government regulators that it disabled, deleted, and/or modified the Third Party Wiretappers' code on the Site and Apps.

59. Plaintiff Jane Doe IV received an email from Kaiser Permanente titled "Notice of Data Breach" dated May 8, 2024 wherein Kaiser recognized and admitted that it had violated Plaintiff's privacy. The email stated that "[o]n 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." The email further acknowledged that the information provided to these Third Party Wiretappers included: "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." The email further stated that, after its investigation into the use of these online technologies, Kaiser Permanente "removed these online technologies from our websites and mobile applications" and also "implemented additional measures with the guidance of experts to safeguard against recurrence of this type of incident."

8. Plaintiff Jane Doe V

60. Plaintiff Jane Doe V is a citizen of Oregon and resides in Beaverton, Oregon.

61. Plaintiff Jane Doe V is a Kaiser Foundation Health Plan member and has received medical treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group since approximately 2010.

62. Plaintiff Jane Doe V has regularly used Kaiser's Site, Patient Portal, and Kaiser Permanente App to access medical information and communicate with her health care providers, including making appointments, researching providers and medical conditions, checking medical results, and reviewing her medical history since approximately 2016.

63. Without Plaintiff Jane Doe V's knowledge or consent, Kaiser allowed the Third Party Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or meaning of the contents of her patient status, identifying information, personal and sensitive health information, and confidential communications with her health care providers through Kaiser's website and mobile application while that information and those messages, reports, and/or communications were in transit from approximately 2016 through approximately November 2023 when Kaiser represented to this Court and government regulators that it disabled, deleted, and/or modified the Third Party Wiretappers' code on the Site and Apps.

64. Plaintiff Jane Doe V received an email from Kaiser Permanente titled "Notice of Data Breach" dated May 14, 2024 wherein Kaiser recognized and admitted that it had violated Plaintiff's privacy. The email stated that "[o]n 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." The email further acknowledged that the information provided to these Third Party Wiretappers included: "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." The email further stated that, after its investigation into the use of these online technologies, Kaiser Permanente "removed these online technologies from our websites and mobile applications" and also "implemented additional measures with the guidance of experts to safeguard against recurrence of this type of incident."

9. Plaintiff Alexis Sutter

65. Plaintiff Alexis Sutter ("Sutter") is a citizen of Virginia and resides in Annandale, Virginia.

66. Plaintiff Sutter is a Kaiser Foundation Health Plan member and has received medical treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group since January of 2022, and prior to that from 2007 through 2012.

67. Plaintiff Sutter has regularly used Kaiser's Site, Patient Portal, and Kaiser Permanente App to access medical information and communicate with her health care providers, including making appointments, reviewing and ordering prescriptions; researching providers and medical conditions, checking medical results, and reviewing her medical history since approximately December 2007, including from January 2022 through the present.

68. Without Plaintiff Sutter's knowledge or consent, Kaiser allowed the Third Party Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or meaning of the contents of her patient status, identifying information, personal and sensitive health information, and

confidential communications with her health care providers through Kaiser's website and mobile application while that information and those messages, reports, and/or communications were in transit from at least January 2022 through approximately November 2023 when Kaiser represented to this Court and government regulators that it disabled, deleted, and/or modified the Third Party Wiretappers' code on the Site and Apps.

69. Plaintiff Sutter received an email from Kaiser Permanente titled "Notice of Data Breach" dated May 8, 2024 wherein Kaiser recognized and admitted that it had violated Plaintiff's privacy. The email stated that "[o]n 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." The email further acknowledged that the information provided to these Third Party Wiretappers included: "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." The email further stated that, after its investigation into the use of these online technologies, Kaiser Permanente "removed these online technologies from our websites and mobile applications" and also "implemented additional measures with the guidance of experts to safeguard against recurrence of this type of incident."

B. Defendants

70. Defendant Kaiser Foundation Health Plan, Inc. is a health care provider headquartered in Oakland, California.

71. Kaiser Foundation Health Plan, Inc. has an integrated care model, offering both hospital and physician care through a network of hospitals and physician practices operating under the Kaiser Permanente name. Members of Kaiser health plans have access to hospitals and hundreds of other health care facilities operated by Kaiser Foundation Hospitals and Permanente Medical Groups across the United States.

72. Kaiser Foundation Health Plan, Inc. is financially responsible for the payment of medical services provided to its enrollees ("Kaiser Plan Members")[14] or has accepted such financial responsibility under contract with one or more of the Kaiser entities. Kaiser Foundation Health Plan, Inc. is the largest health care service plan in the United States, with over 12.7 million members in eight states (California, Colorado, Georgia, Hawaii, Maryland, Oregon, Virginia, Washington, and the District of Columbia) (collectively, the "Kaiser Operating States"). Kaiser Foundation Health Plan, Inc. owns and operates the Site and Apps through which Kaiser Plan Members can provide and access information and perform certain tasks related to their insurance and healthcare.

73. Kaiser Foundation Hospitals is a non-profit, public-benefit corporation headquartered in Oakland, California. Kaiser Foundation Hospitals operates nearly 40 acute care hospitals and 680 medical offices throughout the Kaiser Operating States, with its largest presence being in California, where the majority of its hospitals are located, and a significant presence in Washington with more than 35 facilities throughout Western Washington and the Spokane area. Kaiser Foundation Hospitals employs more than 21,000 physicians, representing all medical fields.

74. Although the Terms and Conditions for the Site and Apps state that the Site and Apps are owned and operated by Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals was also involved in the development and operation of the Site and Apps, for example entering into and executing contracts with certain Third Party Wiretappers, such as Quantum Metric, Adobe, and Dynatrace regarding technologies used on the Site and Apps.

75. Kaiser Foundation Health Plan of Washington is incorporated in Washington and has its principal office in Seattle, Washington. KFHPW Holdings is the sole member of Kaiser Foundation Health Plan of Washington. Kaiser Foundation Health Plan, Inc. is the sole member of KFHPW Holdings.

76. Although the Terms and Conditions for the Site and Apps state that the Site and Apps are owned and operated by Kaiser Foundation Health Plan, Inc., Kaiser Foundation Health Plan of Washington was also involved in the development and operation of certain aspects of the Site and Apps, for example entering into and executing contracts with certain Third Party Wiretappers, such

[14] "Kaiser Plan Members" includes former and current Kaiser Plan Members.

as Adobe, regarding technologies used on the Site and Apps. [redacted].

77. Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and The Permanente Medical Group, Inc. (which is headquartered in Oakland, California and is comprised of physician owned, for profit, partnerships and professional corporations) operate under the name "Kaiser Permanente," which is not a legal entity but a registered trademark or trade name that Kaiser Foundation Health Plan, Inc. owns and Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, The Permanente Medical Group, Inc. and their affiliates use, acting in concert.

III. JURISDICTION AND VENUE

78. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 because this suit is brought under the laws of the United States, specifically the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq*. This Court also has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2) because this a proposed class action in which there are at least 100 Class Members, the matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000, and a member of the Class is a citizen of a different State than Defendant.

79. This Court also has supplemental jurisdiction over the state common law and statutory claims pursuant to 28 U.S.C. § 1367, as these claims are so related to the federal statutory claims over which this Court has original jurisdiction, that they form part of the same case or controversy.

80. This Court has general personal jurisdiction over Defendants because Defendants have sufficient minimum contacts with this District in that they operate and market their services throughout the region and in this District. Further, this Court has personal jurisdiction over Defendants because Defendants are headquartered in this District.

81. Venue properly lies in this District pursuant to 28 U.S.C. § 1391(a), (b), and (c) because: a substantial part of the events or omissions giving rise to Plaintiffs and the Classes' claims

occurred in this District, Defendants conduct a substantial amount of business in this District, and Defendants are headquartered in this District.

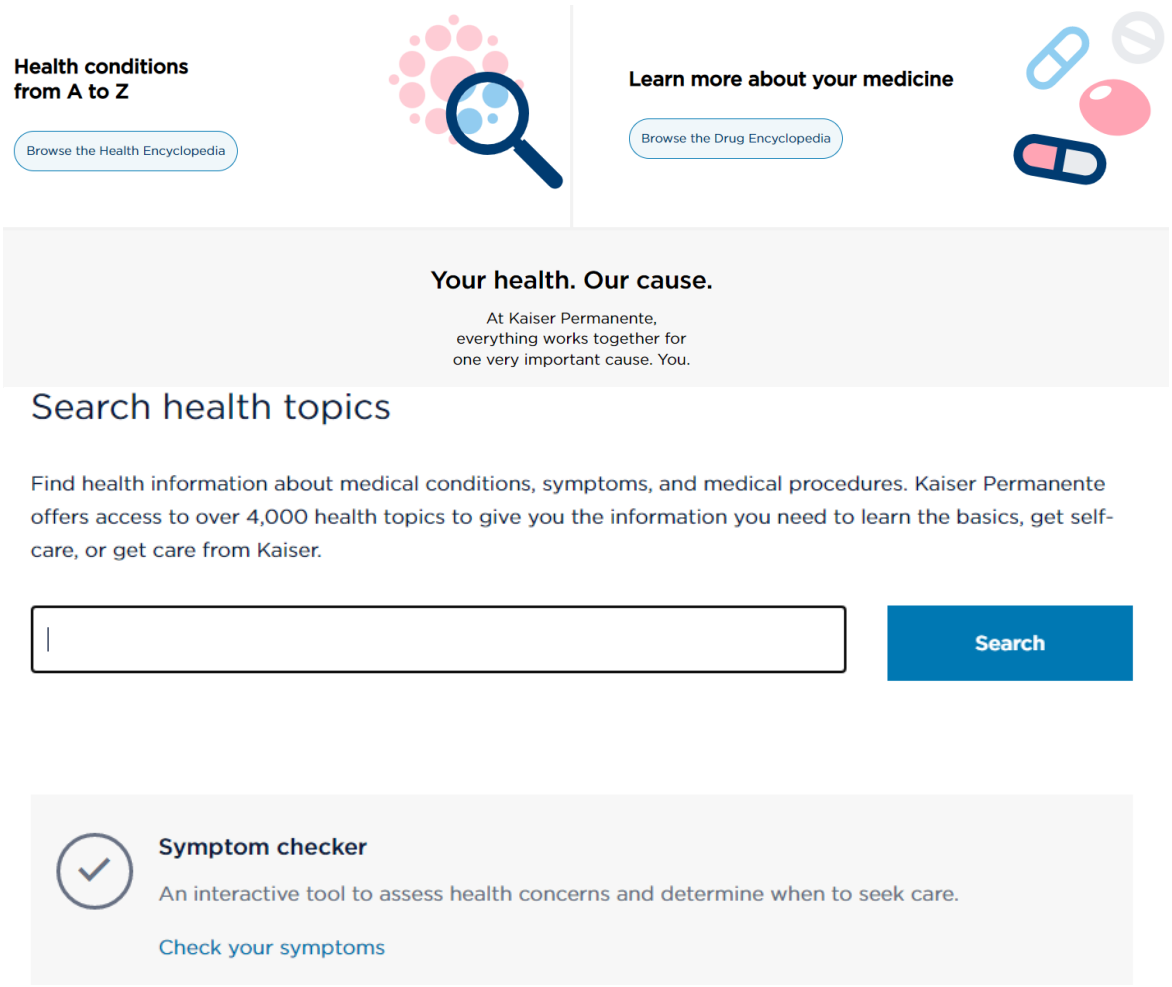
IV. FACTUAL ALLEGATIONS

A. Kaiser Permanente Communicates with Kaiser Plan Members Through the Site and Apps

82. Plaintiffs and members of the Classes are Kaiser Plan Members.

83. Kaiser operates a website ("Site"), with a homepage located at https://healthy.kaiserpermanente.org/front-door ("Homepage"), through which Kaiser Plan Members can perform various tasks that traditionally were only available by physically visiting their health care providers' offices or speaking directly to their health care providers, such as scheduling appointments; checking medical results; reviewing medical histories; researching doctors, locations, and medical services; communicating with providers and paying medical bills.

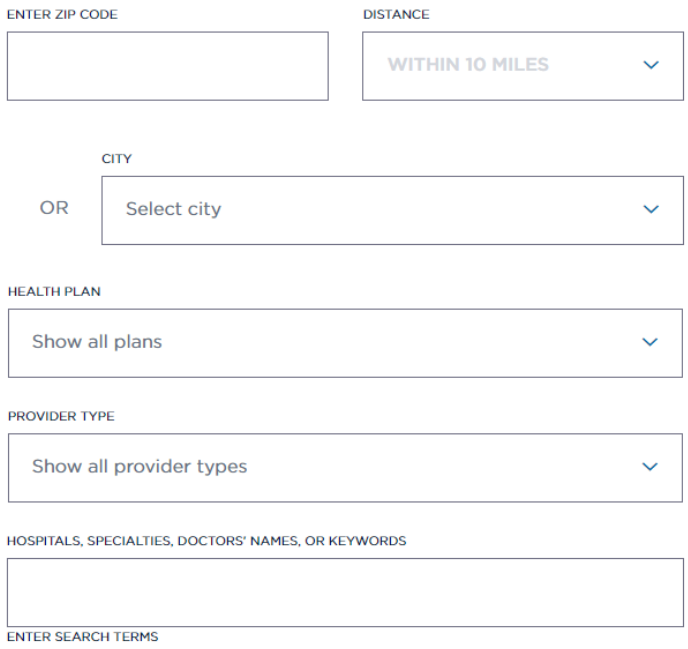
84. The Site's Homepage provides Kaiser Plan Members and the public with information about the health care services that Kaiser Permanente offers, including links to find doctors and locations, get information about health conditions, and learn more about prescribed medicines.



85. For example, on the Homepage, Kaiser Plan Members can click "Browse Health Encyclopedia" and access a page that allows them to find health information about certain medical conditions, symptoms and medical procedures, including over 4,000 health topics, by typing their health-related information into a search form. Kaiser Plan Members can also check their symptoms with an interactive "symptom checker" and "determine when to seek care."

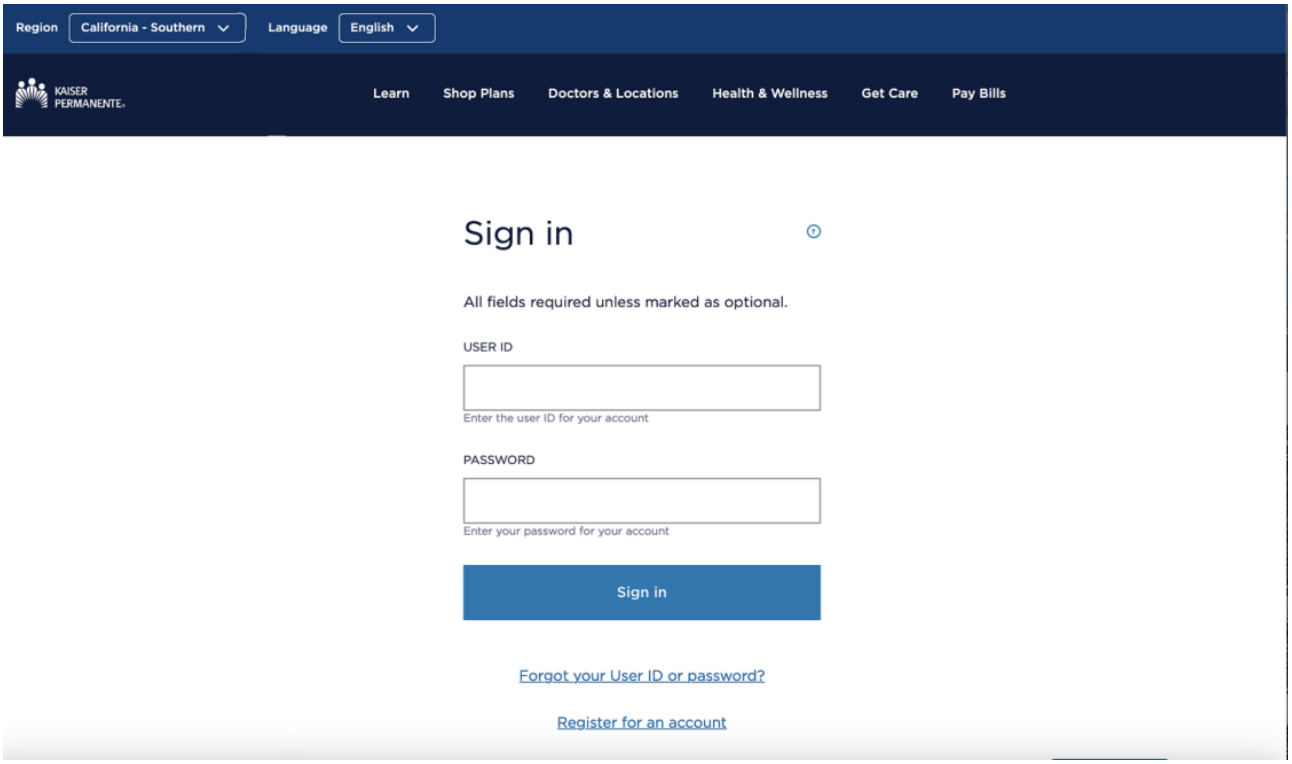
86. As the Site states, these topics and medical information provide Kaiser Plan Members with the information needed to "learn the basics, get self-care, or get care from Kaiser."

87. On the Homepage, Kaiser Plan Members can also click "Find a doctor or location" and access a form (for example at https://healthy.kaiserpermanente.org/southern-california/doctors-locations#/search-form) where they can input their personal and health information to search for health care providers, including by location, specialty, or provider type or with particular keywords related to medical conditions or symptoms the Kaiser Plan Member is experiencing.[15]

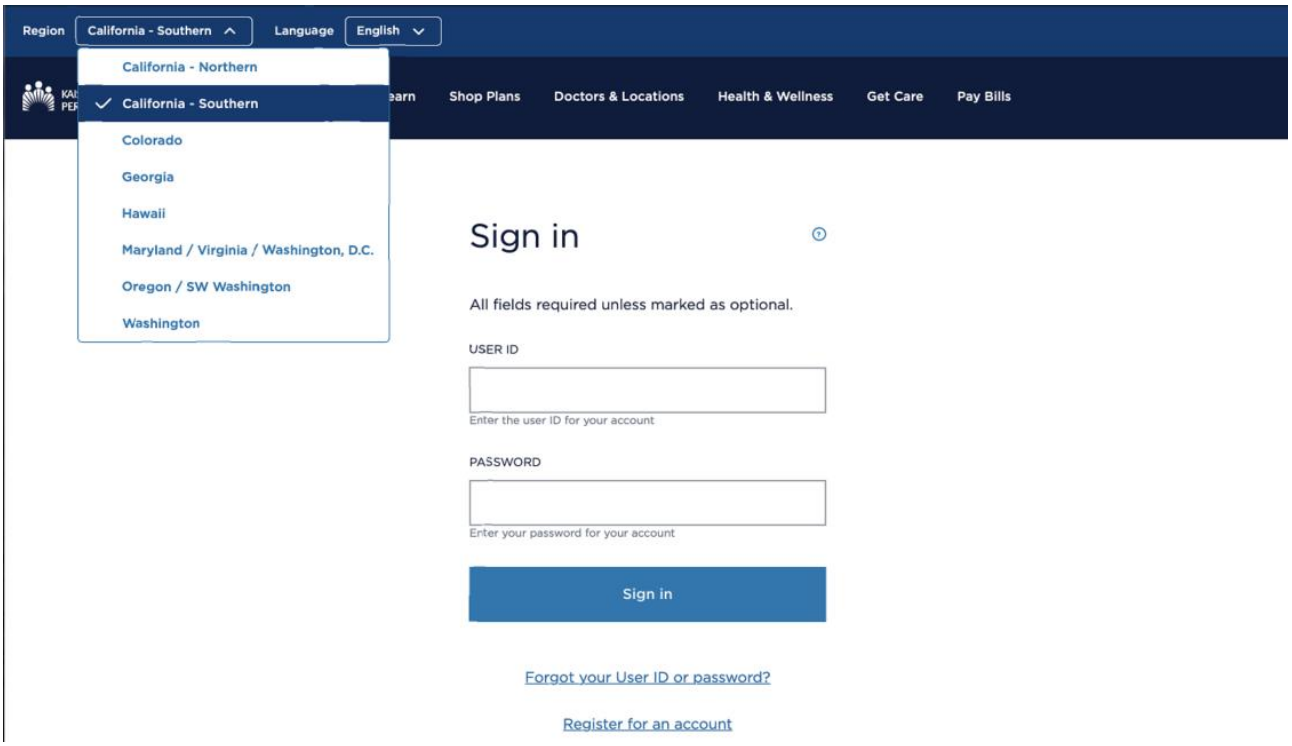


88. Kaiser Plan Members can also access their medical information, prescription information and test results, make payments for healthcare, schedule appointments, order prescriptions, communicate with providers, and perform other actions related to their healthcare after clicking the "Sign In" link for their region ("Portal Login Page") and accessing a purportedly secure patient Portal (the "Portal"). For example, if the Kaiser Plan Member, like Plaintiff John Doe, is located in Southern California, they can select "California – Southern" from a "Region" pulldown menu, click the "Sign In" link and be taken to the Portal Login page for Southern California located at https://healthy.kaiserpermanente.org/southern-california/consumer-sign-on#/signon:

[15] The doctor search functions for the other Kaiser Operating States and regions can be accessed at similarly named page, such as: https://healthy.kaiserpermanente.org/northern-california/doctors-locations#/simple-form.

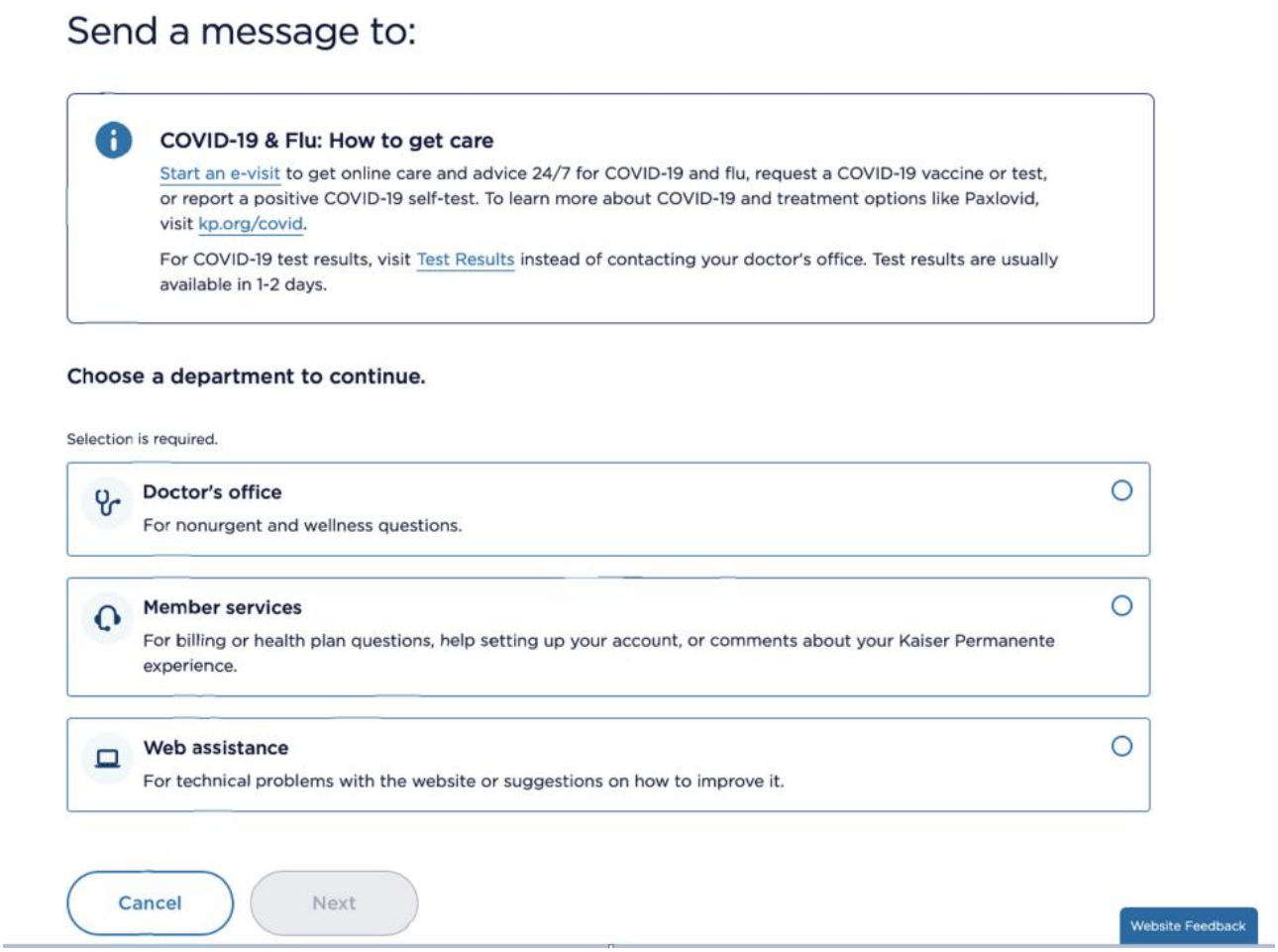

Region
California - Southern
Language
English
KAISER PERMANENTE
Learn
Shop Plans
Doctors & Locations
Health & Wellness
Get Care
Pay Bills
Sign in
All fields required unless marked as optional.
USER ID
Enter the user ID for your account
PASSWORD
Enter your password for your account
Sign in
Forgot your User ID or password?
Register for an account

89. Kaiser Plan Members in Northern California, or other Regions such as Colorado, Georgia, Hawaii, Maryland/Virginia/Washington, D.C., Oregon/ S.W. Washington, and Washington can similarly select their region from a pulldown menu and access their Portal Login Page:

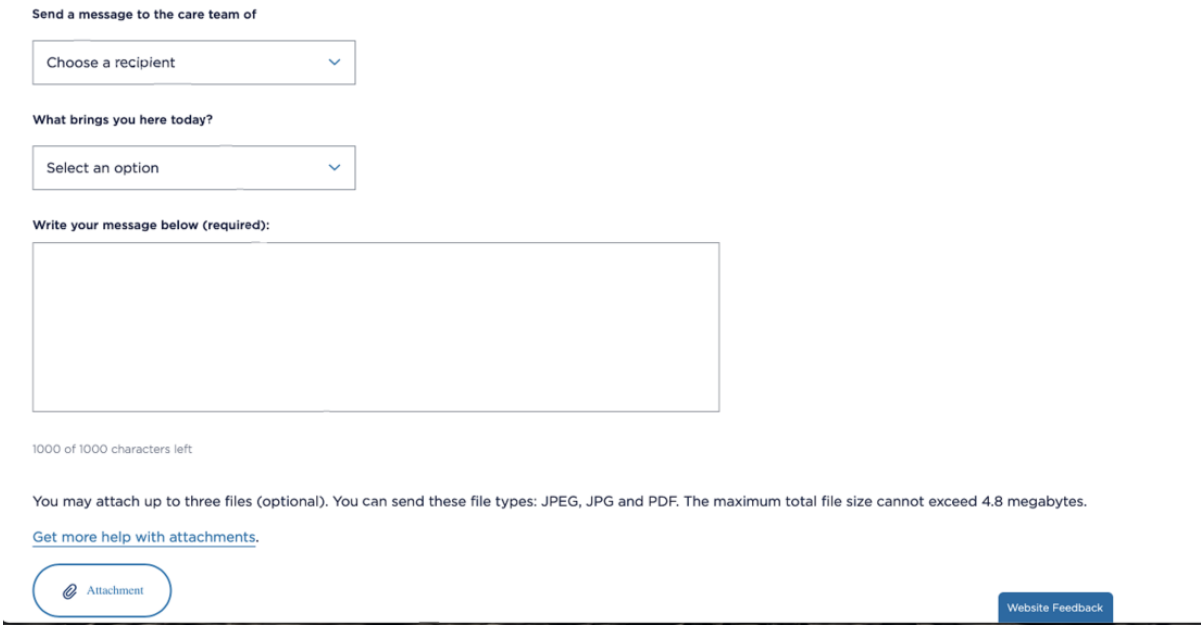


90. After signing into the Portal Login Page and entering the Portal, Kaiser Plan Members can access an array of services and view and provide personal and highly sensitive medical information, including viewing medical history, prescriptions, test results, scheduling appointments, performing online medical evaluations, researching symptoms, and communicating with providers, among other things.

91. For example, the Portal contains a "Message Center" that allows Kaiser Plan Members to communicate directly with their health care providers:



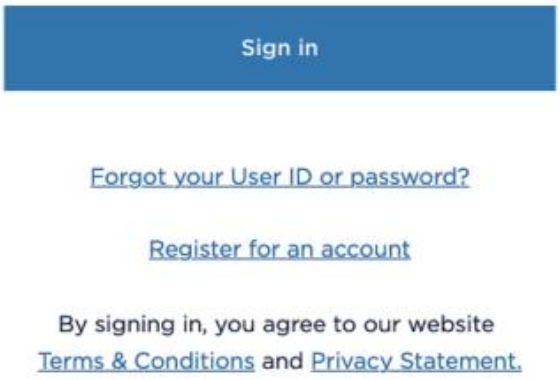
92. After selecting a particular department, Kaiser Plan Members can identify specific recipients to whom they choose to communicate with and type out messages in a free form "Messages" box, with replies also sent and received within the Message Center.



93. Kaiser Plan Members can also use mobile applications to communicate with their doctor's office, schedule appointments, review information about past appointments, fill or refill prescriptions, view their medical history (including allergies, immunizations, ongoing health conditions, and lab test results), make payments for healthcare, choose a doctor, and receive personalized reminders and health information.

94. For example, Kaiser Plan Members in California, Colorado, the District of Columbia, Georgia, Hawaii, Maryland, Oregon, Virginia, and Southwest Washington can use the "Kaiser Permanente App," offered through the Apple App Store[16] and the Google Play Store.[17] Kaiser Plan Members in Washington outside of Southwest Washington can use the "Kaiser Permanente Washington App," offered through the Apple App Store[18] and the Google Play Store.[19]

95. At the bottom of the Portal Login Page, it provides: "By signing in, you agree to our website Terms & Conditions and Privacy Statement."



96. The Kaiser Permanente App's and the Kaiser Permanente Washington App's (collectively, "Apps") pages on the Apple App Store and Google Play Store also provide that use of Kaiser's mobile applications are governed by Kaiser's Privacy Statement.[20]

---

[16] *Kaiser Permanente*, Apple, https://apps.apple.com/us/app/kaiser-permanente/id493390354 (last visited Dec. 5, 2024).
[17] *Kaiser Permanente*, Google, https://play.google.com/store/apps/details?id=org.kp.m (last visited Dec. 5, 2024).
[18] *Kaiser Permanente Washington*, Apple, https://apps.apple.com/us/app/kaiser-permanente-washington/id445899971 (last visited Dec. 5, 2024).
[19] *Kaiser Permanente Washington*, Google, https://play.google.com/store/apps/details?id=org.ghc.android (last visited Dec. 5, 2024).
[20] *See supra* notes 16-19.

97. The Terms and Conditions, and incorporated Privacy Statement form a separate and discrete agreement, and separate and independent contract, between Users of the Site and Apps and the Kaiser Foundation Health Plan. Indeed, on the first page of the Privacy Statement, Kaiser Foundation Health Plan explicitly acknowledges: "The Site allows ***our members and other users*** to view health-related information, communicate with our practitioners and staff, arrange for clinical and health plan services, and access additional services."[21]

98. By clicking "Sign In" before accessing their healthcare information in the Portal and signing into the Apps, Kaiser Plan Members like Plaintiffs thus enter into an express and/or implied contract with Kaiser Foundation Health Plan regarding the parties' respective rights, responsibilities and obligations governing their conduct on the Site and Apps and information provided on the Site and Apps, with the contract terms detailed by the Kaiser Permanente Terms & Conditions and incorporated policies, like the Privacy Statement.

99. Kaiser Plan Members provide Kaiser Foundation Health Plan with a valuable benefit by agreeing to the Terms & Conditions and Privacy Statement and by agreeing to share their personably identifiable information and access their PHI while using the Site and Apps pursuant to the terms in these documents and resulting contract. In return, Kaiser Foundation Health Plan agrees to abide by the promises it sets forth in the Terms and Conditions and Privacy Statement. Moreover, by using the Portal and Apps, Kaiser Plan Members bestow the additional valuable benefits on Kaiser Foundation Health Plan of: (1) making its provision of healthcare services more efficient, and (2) reducing the costs associated with paying for and managing its members' medical conditions. Importantly, as an integrated managed care consortium, Kaiser Permanente is both a healthcare provider and insurer—thus, it is in a position to realize any savings generated by reducing patient costs.

100. The Kaiser Permanente Terms & Conditions, available via hyperlink[22] when signing into the Portal and Apps, and attached hereto as Exhibit 4, explicitly incorporates the Privacy

[21] *Website and mobile application Privacy Statement*, Kaiser (last revised Oct. 2021), https://healthy.kaiserpermanente.org/southern-california/privacy.

[22] *See, e.*g., *Terms & Conditions for our Website and Mobile Application*, Kaiser (last updated June 2022), https://healthy.kaiserpermanente.org/southern-california/termsconditions.

Statement, providing: "Any personal information you submit to the Site (for yourself or someone else) is governed by our Website and KP Mobile Application Privacy Statement." Notably, the Privacy Statement includes but is not limited to Kaiser's legal obligations concerning its treatment of PHI.

101. The Permanente Privacy Statement, also available via hyperlink[23] attached hereto as Exhibit 5, further assures Kaiser Plan Members that "Kaiser Permanente is committed to protecting the privacy of the users of the Site," that it "will use and disclose your personal information as stated in this Privacy Statement," and that it would abide by other promises regarding the confidentiality and protections of Kaiser Plan Members' communications and data on the Site and Apps. However, as set forth herein, Kaiser breached those promises.

102. Kaiser's website also contains a link to the HIPAA Notice of Privacy Practices, attached hereto as Exhibit 6, which purports to describe how and when Kaiser discloses information covered by HIPAA and makes additional promises that compliment and/or go beyond Kaiser's legal duties in this regard; however, as set forth herein, Kaiser also beached these promises.

103. Significantly, nowhere does Kaiser disclose to Kaiser Plan Members that Kaiser is intercepting, and/or has aided, agreed with, employed, and/or conspired with, third parties that are intercepting and/or recording PHI and other sensitive and confidential information that Kaiser Plan Members are sending, accessing, reviewing, or receiving through the Site, Portal, and Apps with the embedded code and capabilities described herein. Indeed, as reflected in the chart below, which Kaiser produced in discovery (and which Kaiser has been ordered to supplement by December 15, 2024 with the identities of all third-party technologies located on the log-in/authentication portions of the Website and Apps), Kaiser installed a vast array of Third Party Wiretappers' tracking technologies throughout the Site and Apps:

[23] *See, e.g.*, *Website and mobile application Privacy Statement*, Kaiser (last revised Oct. 2021), https://healthy.kaiserpermanente.org/southern-california/privacy.

Vendor	Service/Product Name	Purpose	Location
Adobe	Adobe Target	Platform Support - Site Analytics	KP Site; KP App
Adobe	Adobe Analytics	Platform Support - Site Analytics	KP Site; WA Site; WA App; KP App
Adobe	Adobe (Marketo)	Marketing	KP Site
Adobe	Adobe Audience Manager	Platform Support - Site Analytics	KP Site; WA Site; WA App; KP App
Adobe	Adobe Advertising	Marketing	KP Site; KP App
Dynatrace	Infrastructure and Application Observability	Platform Support - Performance and Support	WA Site; WA App
Google	DoubleClick	Marketing	KP Site; WA Site; WA App; KP App
Google	Google Ads	Marketing	KP Site; WA Site; WA App; KP App
Google	Google Analytics 360	Platform Support - Site Analytics	KP Site; WA Site; WA App; KP App
Google	Google Tag Manager 360	Platform Support - Site Analytics	KP Site; WA Site; WA App; KP App
Google	ReCaptcha	Verification Services	KP Site, WA Site
Google	Google Maps (API)	Google Maps Integration	KP Site, WA Site
Microsoft	Microsoft Conversion Tag (aka Bing Conversion Tag)	Marketing	KP Site; WA Site; KP App
Quantum Metric	Quantum Metric Real User Monitor	Platform Support - Performance and Support - Session-Based Analytics	KP Site; KP App
Twitter	Twitter	Marketing	KP Site; KP App

104. Despite its express and implied assurances of privacy, Kaiser intentionally incorporated the Third Party Wiretappers' code and recording technology on the Kaiser Site and Apps, and allowed the tracking and disclosure of Kaiser Plan Members' individually identifying personal information, PHI, other personal and sensitive health information, and private, sensitive, and confidential communications with Kaiser and its providers to Third Party Wiretappers.

105. Kaiser acted willfully and deceptively by permitting the unauthorized interception, disclosure, and transfer of personally identifying information and private health information in violation of its own Site Terms and Conditions.

106. Kaiser knew that by embedding the Third Party Wiretappers' code, it was disclosing and permitting the Third Party Wiretappers to intercept and collect personally identifying, and personal and sensitive information relating to Kaiser Plan Members' medical treatment and/or PHI that Kaiser was required to protect and safeguard. As detailed herein, the Third Party Wiretappers code intercepts, collects, and transmits significant amounts of healthcare-related communications along with personally identifiable information about Kaiser Plan Members, including IP Addresses, first names, marketing IDs, device identifiers, and other information that alone or in combination can be used to identify the individual Kaiser Plan Members.

107. Indeed, as Kaiser admitted to regulators in or around April 12, 2024, the "information collected by these technologies about Kaiser members may be considered Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), pursuant to recent guidance from the Department of Health and Human Services (HHS)."[24] However, as set forth herein, Kaiser knew that the Third Party Wiretappers' code was intercepting, transmitting, and collecting PHI and other personally identifying information to the Third Party Wiretappers long before the April 12, 2024 disclosure.

108. Kaiser's actions described herein were all intentionally undertaken and knowingly ratified by Kaiser's officers, directors, or managing agents.

B. Multiple Third Party Wiretappers Intercept Kaiser Plan Members' Information Shared with, and Communications with, Kaiser and Its Providers

1. Kaiser Allows Quantum Metric to Intercept Kaiser Plan Members' Information and Communications from the Site and Kaiser Permanente App

109. Unbeknownst to Kaiser Plan Members and against their reasonable expectations, Kaiser allows Quantum Metric to intercept Kaiser Plan Members' personal and sensitive identifying

[24] Pls.' Notice of Kaiser's Disclosures at Ex. A, ECF No. 127-1.

and medical information and confidential communications from the Site, Portal, and Kaiser Permanente App.

110. By at least January 2022, Kaiser placed Quantum Metric's code, including "Session Replay" code, on its Homepage, Portal Login Page, and other pages on the Site—including within the Portal—which intercepts and records the contents of Kaiser Plan Members' information and confidential communications, and sends that information and those communications to Quantum Metric.

111. After Plaintiffs filed their initial Complaint on June 9, 2023, and subsequently moved for a preliminary injunction asking that this Court, *inter alia*, order that Kaiser remove the Third Party Wiretappers' source code embedded in the Site and Kaiser Permanente App that allows the Third Party Wiretappers to intrude upon, read, intercept, and/or use personal identifying and medical information and communications, Kaiser, in November 2023, represented to this Court that it had disabled, deleted, or modified the Quantum Metric code on the Site and Apps. It did not represent that ***all code*** has been removed, nor did it describe how the code had been disabled or modified, and only full discovery can confirm whether all of the tracking code has been removed.

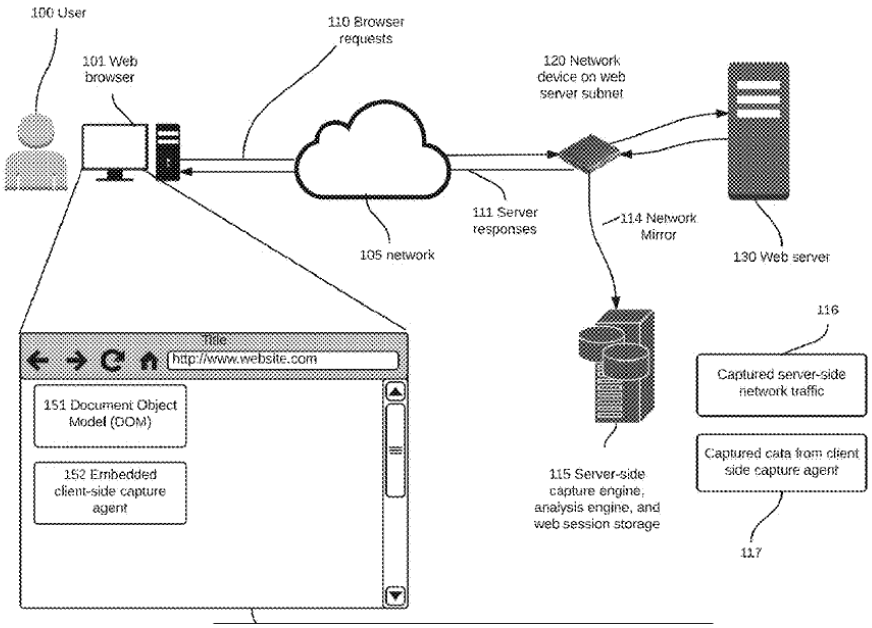
112. Among other functions, Quantum Metric collects and saves website communications, including those on the Site and Portal, through a service named "Session Replay." Session Replay captures internet communications between a website user and a website, including those on the Site and Portal, in real time while those communications are in transit. [redacted].

113. As Quantum Metric explains: "At its core, **session replay** is technology that allows you to watch a user's session as they experienced it, similar to how you watch a video. You can pause, rewind, and fast-forward the session (just like a YouTube video) to watch how a user interacts with a website or mobile app."[25]

[25] *What is Session Replay*, Quantum Metric, https://web.archive.org/web/20240326030132/https://www.quantummetric.com/enterprise-guide-to-session-replay (last visited Dec. 5, 2024).

114. Session replay technologies work by using "embedded snippets of code . . . [that] watch and record a visitor's every move on a website, in real time."[26] This was done on the Site and the Portal when used by Kaiser Plan Members.

115. As illustrated in Quantum Metric's patent, after a user submits a communication to a web server, such as Kaiser's, Quantum Metric's embedded side capture agent code redirects the communications to Quantum Metric's server-side capture engine, analysis engine, and web session storage:



116. From the moment a Kaiser Plan Member loads Kaiser's Site, Quantum Metric is intercepting all of the content viewed and communicated, as well as the Kaiser Plan Member's interactions with the Site, similar to an individual peering over the user's shoulder and listening in on the patient's conversations with their medical provider.

117. As Kaiser Plan Members navigate the Site, including accessing the Portal, the Site makes numerous "POST" calls to Quantum Metric, the size of which changes based on site activity.

118. A "POST" call is a HTTP method that sends user data to a server, usually to create or update a resource on the server. In a POST transmission, data is included in the body of the request, not in the URL, which allows for larger amounts of data to be transmitted compared to other methods.

[26] Tomas Foltyn, *What's the Deal with Session-Replay Scripts?*, welivesecurity (Apr. 20, 2018, 1:40 pm), https://www.welivesecurity.com/2018/04/20/whats-deal-session-replay-scripts/.

Instead of transmitting information about the User's initial request to the server, a POST commands the User's browser to intercept and redirect subsequent communications from the User to the server.

119. As disclosed in the Quantum Metric End-User license agreement, Kaiser allows Quantum Metric to collect, process, store, and display the customer's interactions with Kaiser's website.[27]

120. Kaiser Plan Members' communications are further subject to the company's independent processing, analyses, and use of this session replay data.[28] For example, [redacted].

121. Quantum Metric also allows [redacted].

122. Quantum Metric also [redacted].

123. Quantum Metric also [redacted] As Quantum Metric explains on its website, "[t]he Technology Partner Program enables technology companies to build, test, and certify integrations with the Quantum Metric platform. The program provides tools and resources, as well as sales and marketing benefits, to extend your market reach."[29]

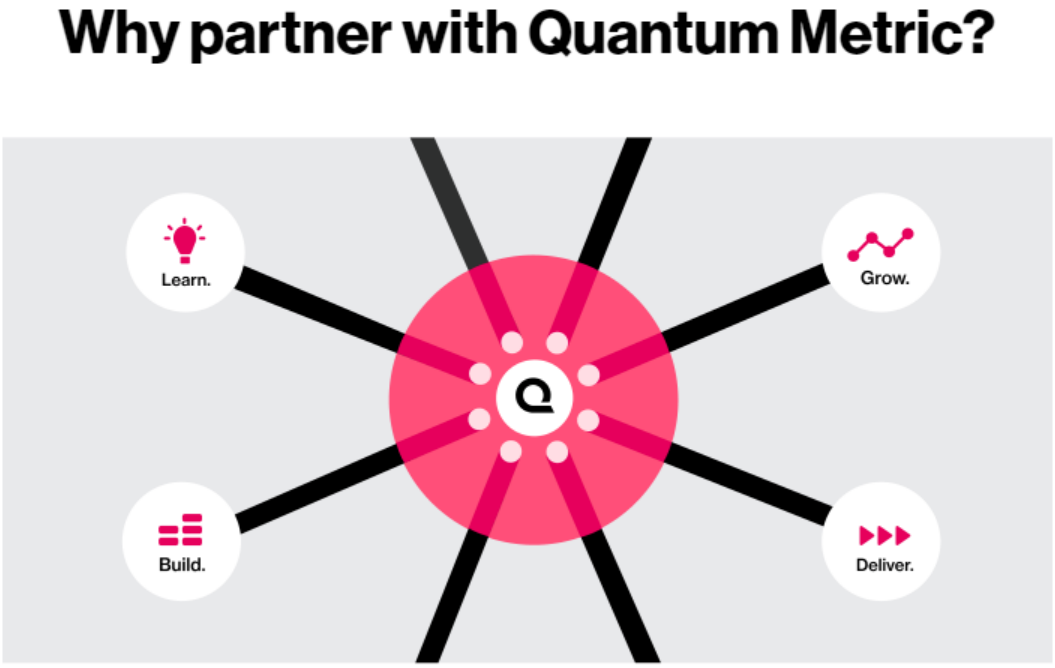
124. Quantum Metric's "Solution Partners include system integrators, digital agencies, resellers, referral and fulfillment partners. The Solution Partner Program enables partners to develop and deliver specialized solutions and services with Quantum Metric and provides co-sell incentives

[27] *SaaS End-User License Agreement*, Quantum Metric (last modified Nov. 13, 2024), https://iam.quantummetric.com/terms-and-conditions ("Subject to the terms of the Agreement, Quantum is provided a limited license to Customer Data for the purpose of providing the Quantum Service, including a license to ***collect, process, store, and display*** Customer Data to the extent appropriate in providing the Quantum Service to Customer.").

[28] *See, e.g.*, *What Is Session Replay* at 6, Quantum Metric, https://www.quantummetric.com/enterprise-guide-to-session-replay/ (last visited Dec. 5, 2024) ("More advanced session replay tools can ***automatically identify*** the friction and where it occurred in an application, ***segment all users*** that experienced that friction, and ***quantify the loss in conversion and revenue***.").

[29] *Why Partner with Quantum Metric?*, Quantum Metric, https://www.quantummetric.com/partners/ (last visited Dec. 5, 2024).

to accelerate partner business growth." Quantum Metric promotes its partner networks as a hub and spoke design, with Quantum Metric in the center, with the various partners located along the spokes, which get and share information through Quantum Metric serving as the hub.



125. Quantum Metric also uses Kaiser Plan Members' communications for its own research and analysis purposes, continuing to build and refine its products for its own profit.[30]

126. [redacted]

[redacted]

[redacted]

[30] *See SaaS End-User License Agreement*, Quantum Metric (last modified Nov. 13, 2024), https://iam.quantummetric.com/terms-and-conditions.("Quantum may use certain Aggregated Data in order to perform analysis and statistical reporting and for auditing, research and analysis to operate and improve Quantum technologies and services.").

[redacted]

127. [redacted]

128. At a minimum, Quantum Metric's Session Replay captured Kaiser Health Plan Members' status as Kaiser patients when they logged into the Portal, which when coupled with the personally identifiable information that Kaiser admits is transmitted to Quantum Metric, constitutes protected health information under HIPAA.

129. Moreover, the nature of the information displayed inside the Portal and captured through Session Reply necessarily includes protected health information, as the Portal is where Kaiser Plan Members access their medical records, test results, schedule appointments, exchange messages with their health care providers, and engage in other sensitive healthcare communications.

130. In fact, [redacted]

131. Instead, [redacted]

[redacted].

132. [redacted]

133. It was not until November 2023, after Plaintiffs filed this lawsuit and moved for a preliminary injunction to force Kaiser to remove the offensive code from its Site and Apps—which caused Kaiser to disable, delete or modify the code on its Site and Apps—that Kaiser [redacted]

134. Thus, by installing the Quantum Metric code on its website, Kaiser allowed Quantum Metric to intercept and record Kaiser Plan Members' identifying information, personal and sensitive medical information, including PHI, HIPAA-protected health information, and confidential communications in real time.

135. On information and belief, Kaiser has continually allowed Third Party Wiretappers to intercept Plaintiffs' and other Kaiser Plan Member's personal information from at least January 2022 until approximately November 2023 when Kaiser represented to this Court that it had disabled, deleted, or modified the Quantum Metric code on the Site and Apps.[31]

136. By way of example, on May 31, 2023, after Plaintiff Jane Doe logged into the Portal—which displayed her Name, Medical Record Number (Kaiser ID #), Region, and Coverage Status—

[31] *See* Declaration of Bill Vourthis, ECF No. 96.

but performed no further activities, the amount of data intercepted and transferred to Quantum Metric (at kp-app.quantummetric.com) was about 260 bytes. Thereafter, when Plaintiff Jane Doe performed several activities within the Portal, the amount of the data transferred to Quantum Metric increased to over 102 kB, indicating that her activity inside the Portal was being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com. This signifies that Jane Doe's communications within the Portal was being captured by Session Replay and intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

137. After Plaintiff Jane Doe logged into the Portal and then accessed the Doctor Search Page and performed no further activities, the amount of data intercepted and transferred to Quantum Metric was 311 bytes. Thereafter, when Plaintiff Jane Doe entered personal medical search information into the Doctor Search page, the amount of data transferred to Quantum Metric increased to over 122 kB, similarly indicating that Plaintiff Jane Doe's medical search information was being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

138. Kaiser allowed Quantum Metric to intercept similar information from Jane Doe every time she logged-in since Quantum Metric's code was first installed on the Site and similarly allowed Quantum Metric to intercept log-in information for Plaintiffs John Doe, John Doe II, John Doe III, Jane Doe II, Jane Doe III, Jane Doe IV, Jane Doe V, Alexis Sutter and other members of the Classes.

139. For example, on June 6, 2023, when Plaintiff John Doe logged into the Portal and accessed recent medical test results, the amount of data transferred to Quantum Metric was over 85 kB, indicating that information about Plaintiff John Doe's personal and sensitive identifying and medical information, and private and confidential medical test results, was also being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

140. On information and belief, the same type of information tracked, disclosed, and sent to Quantum Metric for Plaintiffs has been tracked, disclosed, and sent to Quantum Metric for other members of the Classes.

141. Additionally, when Kaiser Plan Members navigate other portions of the Site, Quantum Metric intercepts and receives that content as well. For example, if a patient searches for doctors who specialize in Addiction Medicine, Quantum Metric will receive the search results displaying this

sensitive information, as well as data regarding all of the information the Kaiser Plan Members provided and received regarding that topic.

142. In addition, when Plaintiff Jane Doe accessed her bill pay account, the amount of data transferred to Quantum Metric was over 84 kB, indicating that information about Plaintiff Jane Doe's personal and sensitive identifying health related financial information was also being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

143. When Plaintiff John Doe participated in a Social Health Review inside the Portal the amount of data transferred to Quantum Metric was over 25 kB, indicating that information about Plaintiff John Doe's personal and sensitive identifying and medical information, and private and confidential medical test results, was also being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

144. When Plaintiff John Doe accessed the Message Center inside the Portal, the amount of data transferred to Quantum Metric was over 330.7 kB, indicating that information about Plaintiff John Doe's personal and sensitive identifying and medical information, and private and confidential medical test results, was also being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

145. When Plaintiff John Doe accessed his Medical Summary inside the Portal, the amount of data transferred to Quantum Metric was over 25 kB, indicating that information about Plaintiff John Doe's personal and sensitive identifying and medical information, and private and confidential medical test results, was also being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

146. When Plaintiff John Doe accessed his bill pay account, the amount of data transferred to Quantum Metric was over 84 kB, indicating that information about Plaintiff John Doe's personal and sensitive identifying health related financial information was also being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

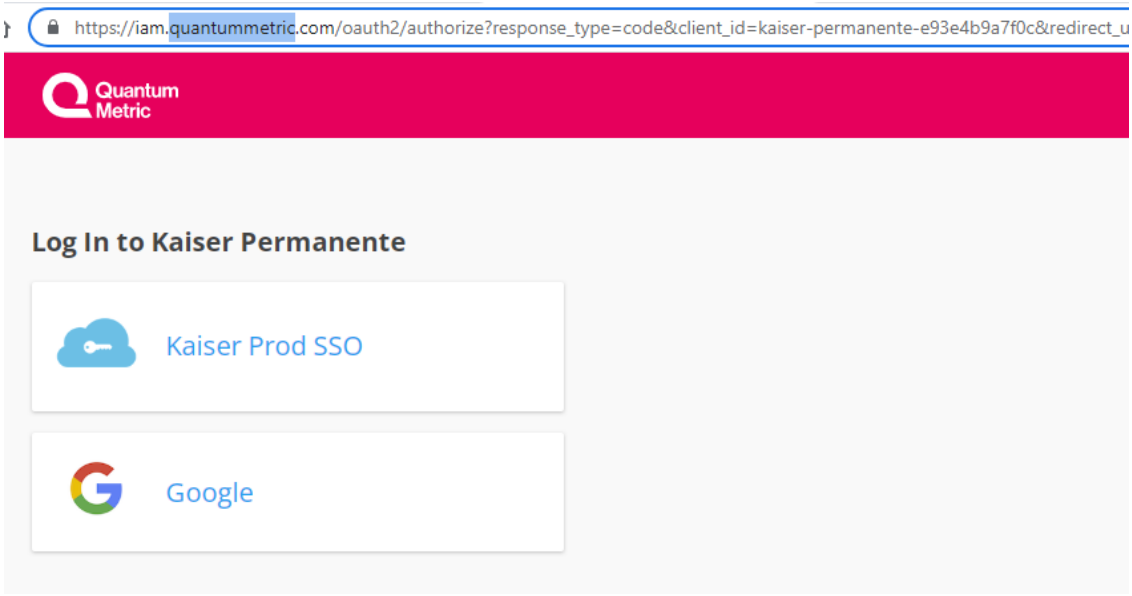
147. When Plaintiff John Doe logged out of the Portal and conducted a search for a neurologist on the Site, the amount of data transferred to Quantum Metric was over 427.1 kB, indicating that information about Plaintiff John Doe's personal and sensitive identifying and medical

information, and private and confidential medical test results, was also being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

148. When Plaintiffs John Doe II, John Doe III, Jane Doe II, Jane Doe III, Jane Doe IV, Jane Doe V, and Alexis Sutter accessed the Kaiser website and Patient Portal, their communications were similarly intercepted by Quantum Metric.

149. On information and belief, the communications of members of the Classes who accessed the Kaiser website and Patient Portal were also intercepted by Quantum Metric.

150. The recordings of Plaintiffs and other Class Members' information and confidential communications on the Site are saved on Quantum Metric's systems and are available for viewing on Quantum Metric's website, an example of which is below:



151. Kaiser voluntarily embedded Quantum Metric's software code on the Site, knowing that Quantum Metric's software would intercept, record, and redirect Kaiser Plan Members' Site and Portal activity, including personal health information and/or HIPAA-protected information and communications with Kaiser and its providers.

152. While Quantum Metric's documents show that Quantum Metric is also collecting analytics data, the Quantum Metric Session Replay recording technology utilized by Kaiser is intended to record and playback individual browsing sessions, as well as the private and confidential information and communications shared in those sessions. The monitoring that Quantum Metric's

technology provides extends beyond the computer "cookies" with which ordinary consumers may be familiar and is not disclosed anywhere in the Privacy Statement.

153. Moreover, the collection and storage of Kaiser Plan Members' communications with their health care providers may cause sensitive health information and other personal information displayed on a page to leak to additional third parties. This may expose Kaiser Plan Members who use the Site and/or Portal to identity theft, online scams, and other unwanted behavior.

154. In a 2017 study by Princeton University's Center for Information Technology Policy concerning session recording technologies, the researchers noted "[c]ollection of page content by third party replay scripts may cause sensitive information such as medical conditions, credit card details and other personal information displayed on a page to leak to the third party as part of the recording. This may expose users [like Plaintiffs and members of the Classes] to identity theft, online scams, and other unwanted behavior."[32]

155. The study goes on to state that "the extent of data collected by these services far exceeds user expectations; text typed into forms is collected before the user submits the form, and precise mouse movements are saved, all without any visual indication to the user. This data can't reasonably be expected to be kept anonymous."[33]

156. As deployed, on the Site and Kaiser Permanente App, Quantum Metric's code, including its Session Replay recording function and other code, as employed by Kaiser, functioned as a wiretap, and Quantum Metric acts as a third party wiretapper.

157. Kaiser purposefully collected Plaintiffs' and Class Members' personally identifiable information while also installing Quantum Metric's code on its website and mobile applications and failing to prevent and/or aiding and abetting in that personally identifiable information being intercepted by Quantum Metric thereby compromising Plaintiffs' and Class Members' privacy and the confidentiality of their personally identifiable information. Thus, by allowing Quantum Metric to

[32] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

[33] *Id.*

intercept Kaiser Plan Members' information and communications from the Site and Apps, Kaiser foreseeably harmed Plaintiffs and similarly situated Class Members.

158. Defendants knew or should have known that they were failing to comply with the applicable statutes and common law duties governing their conduct, and that Defendants' breach would cause Plaintiffs and Class Members to experience foreseeable harms associated with the unauthorized interception, disclosure, and use of their personal health information by Quantum Metric.

2. Kaiser Allows Adobe to Intercept Kaiser Plan Members' Information and Communications from the Site and Apps

159. Unbeknownst to Kaiser Plan Members and against their reasonable expectations, Kaiser allows Adobe to intercept Kaiser Plan Members' information and communications from the Site and Apps, including inside the Portal.

160. Since at least 2015, Kaiser has allowed Adobe to intercept Kaiser Plan Members' personal and sensitive identifying and medical information, PHI, and private and confidential communications, including through code connected with the Adobe Experience Cloud a/k/a Adobe Marketing Cloud service embedded on the Site, including within the Portal, and with other technology such as LifeCycle and Marketo products since at least 2012, which later became integrated with the Adobe Marketing Cloud service. The Adobe Experience Cloud service is a suite of products offered by Adobe, which allow businesses to personalize and improve their marketing on websites, apps, and social media pages by collecting and analyzing information about website visitors.

161. The Adobe Experience Cloud includes a number of services including: Measurement solutions, which allows companies to measure and understand visitors who use their websites, apps, and social media pages, as well as how they interact with online marketing campaigns; Personalization solutions, which allows companies to test new content and make their websites, apps, social media pages, and emails more relevant to particular visitors; Content management solutions, which allows companies to store, update, and deliver images and other content on their websites, within their apps, and in online marketing materials; and Advertising solutions, which allows companies to improve their online advertising on websites, apps, search engines, and social media,

including helping companies send emails, text messages, and other online and offline marketing campaigns.[34]

162. The Adobe Experience Cloud collects an array of personal and personally identifiable information about website visitors, including:

- Where you go and what you do on that company's websites, apps, or social media pages
- Your web browsing activity, including the URLs of the company's web pages you visit
- The URL of the page that displayed the link that you clicked on, which brought you to that company's website
- The web search you performed that led you to that company's website
- Information about your web browser and device, such as device type, browser type, advertising identifier, operating system, connection speed, and display settings
- Your IP address (or partial IP address, depending on how the company has configured the solution), which may be used to approximate your general location
- Location information from your mobile device or web browser
- Social media profile information
- Information you may provide on that company's website, app, or when interacting with that company's social media pages, such as information you provide on registration forms
- Ad campaign success rates, such as whether you clicked on a company's ad and whether viewing or clicking on the ad led to your purchase of that company's product or service
- Items you've purchased or placed in your shopping cart on that company's website or app[35]

163. As part of the Adobe Advertising Cloud solution, Adobe makes available, certain health-related segments supplied by third party data providers to the companies using the Adobe Advertising Cloud, allowing companies to use these segments to target ads when they are using the Adobe Experience Cloud. These data segments generally fall into the following categories: (1) occupation in a health-related field, (2) health related topics and conditions, (3) interest in health

[34] *Adobe Experience Cloud privacy*, Adobe (last updated Dec. 5, 2022), https://www.adobe.com/privacy/experience-cloud.html.
[35] *Id.*

insurance, (4) diet, fitness, weight-loss, and healthy lifestyles, (5) consumer goods and services for personal healthcare, vision care, grooming, and beauty, (6) over the counter medicines, remedies, and dietary supplements, and (7) health related charities.

164. [redacted] however, Kaiser nonetheless allowed Adobe to intercept its Kaiser Plan Members' personally identifiable information and confidential medical communications, including PHI, through various Adobe products offered through and connected to the Adobe Experience Cloud.

165. [redacted].

166. [redacted],

[36] [redacted].

[37] *Experience Cloud audiences*, Adobe (Apr. 25, 2024), https://experienceleague.adobe.com/en/docs/core-services/interface/services/audiences/audience-library.

[redacted].[38]

167. [redacted]

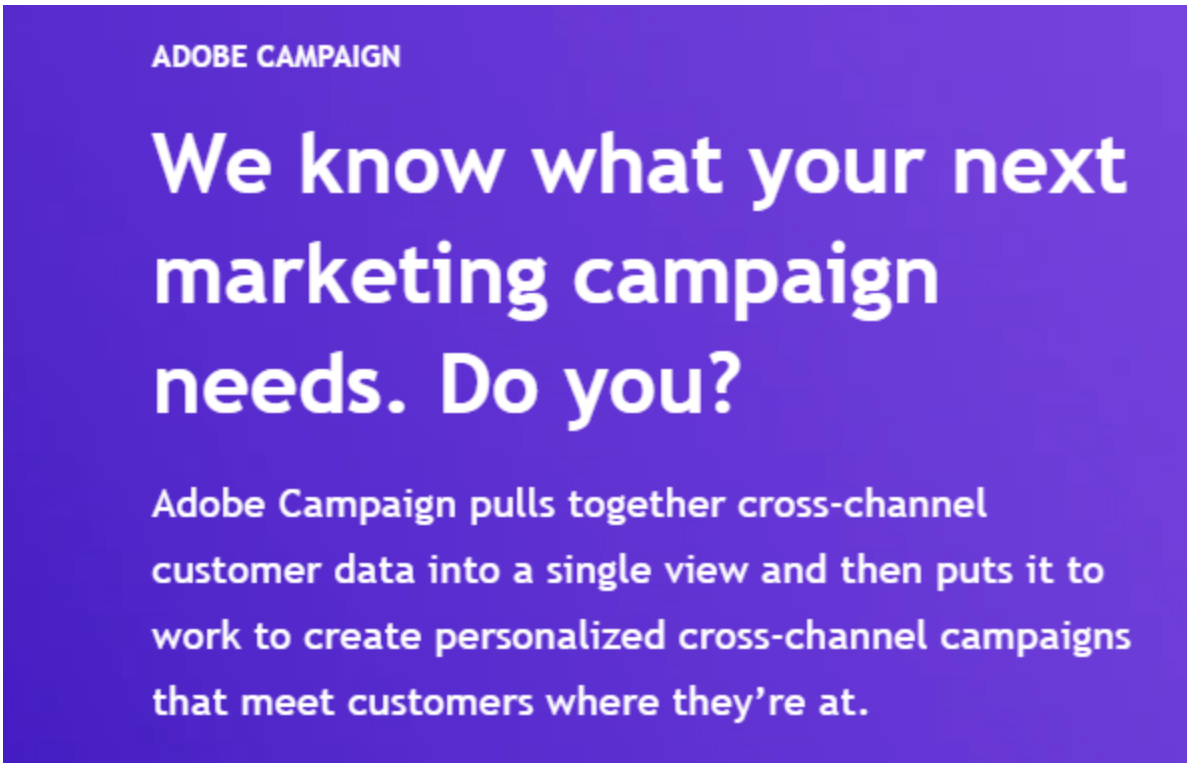
168. [redacted]

169. Adobe Campaign "pulls together cross-channel customer data into a single view and then puts it to work to create personalized cross-channel campaigns that meet customers where they're at."[40] As Adobe promotes on its website, Adobe knows more information about you than you know about yourself:

[38] [redacted].

[39] [redacted]

[40] [redacted]



170. [redacted]

[redacted]

171. [redacted]

172. When visiting the Site and Apps, the Adobe Experience Cloud collects Kaiser Plan Members' information through an array of tracking technologies, including cookies and/or web beacons (also known as tags or pixels), such as the third party cookies omtrdc.net, demdex.net, and the Adobe Experience Platform Launch, which delivers a library containing specified tags for other Adobe Experience Cloud solutions.[41] Upon information and belief, these cookies are specific identifiers used by Adobe for cookie-syncing and mapping, a process described below in Section IV(F). For example when Jane Doe II logged in to the Portal, the everest_g_v2 cookie value and its g_surferid ("everest_g_v2=g_surferid~**ZP91XgAAAHLjaQNz**") was, upon information and belief, sent to "https://dpm.demdex.net/ibs:dpid=411&dpuuid=**ZP91XgAAAHLjaQNz"**.

173. As Kaiser Plan Members navigate the Kaiser Site and Apps, the code embedded on the Site and Apps commands Kaiser Plan Members' browsers to make numerous "POST" calls which send information about Kaiser Plan Members' personally identifying information, PHI and confidential communications with Kaiser that are intercepted by Adobe.

[41] This includes cookies identified as "everest_g_v2" and "demdex.net", which aid in tracking users. According to Adobe's marketing materials, the everest_g_v2 cookie is "created after a user initially clicks a client's ad, and used to map the current and subsequent clicks with other events on the client's website."

174. Adobe has established subdomains on its own server, such as the subdomain kaiser.tt.omtrdc.net on Adobe's omtrdc.net server, where Adobe receives and stores the communications intercepted from Kaiser.[42]

175. [redacted]

176. [redacted]

177. [redacted]

178. [redacted].

[42] *Adobe Experience Cloud privacy*, Adobe (last updated Dec. 5, 2022), https://www.adobe.com/privacy/experience-cloud.html.

179. [redacted]

180. [redacted]

181. Moreover, even after [redacted] Kaiser continued to send and allow Adobe to intercept Plaintiffs' and other Kaiser Plan Members' personally identifying information and PHI on the Site and Apps until approximately November 2023 when Kaiser represented to this Court that it had disabled, deleted, or modified the Adobe code on the Site and Apps.

182. For example, on June 6, 2023, after Plaintiff John Doe logged into the Portal, the following data was intercepted by Adobe and sent to Adobe's server at the kaiser.tt.omtrdc.net subdomain, which as detailed below shows that Adobe received a host of personally identifiable health information, including: user data (color coded in blue), the URL of the Website the user is currently browsing (color coded in green), unique IDs (color coded in yellow), customer IDs and

status values (color coded in grey),[43] and segmentation values that enable the Website to show personalized content (no color).

{"requestId":"d65c5d634b7d484a9176516962af4071","context":{"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36","clientHints":{"mobile":false,"platform":"macOS","browserUAWithMajorVersion":"\"Google Chrome\";v=\"113\", \"Chromium\";v=\"113\", \"Not-A.Brand\";v=\"24\""},"timeOffsetInMinutes":-420,"channel":"web","screen":{"width":1512,"height":982,"orientation":"landscape","colorDepth":30,"pixelRatio":2},"window":{"width":1512,"height":871},"browser":{"host":"healthy.kaiserpermanente.org","webGLRenderer":"ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)"},"address":{"url":"https://healthy.kaiserpermanente.org/southern-california/secure/inner-door","referringUrl":"https://healthy.kaiserpermanente.org/southern-california/consumer-interrupt.html"}},"id":{"tntId":"[redacted]","thirdPartyId":"[redacted]","marketingCloudVisitorId":"[redacted]","customerIds":[{"id":"[redacted]","integrationCode":"kpaamidepp","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"kpaamidudr","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"kpaamid_One-off-datasets","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"pzn_crm","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"mbox3rdPartyId","authenticatedState":"authenticated","type":"DS"}]},"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"01AFA18961CACA34-2D8CDB5E307D31FB"}},"execute":{"pageLoad":{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:secure:inner-door","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":7692006,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg101v":27,"Seg516e":false,"Seg126v":false,"modval":6,"Seg21":100453,"Seg22":"","Seg24":"urn:kp:prodiem","Seg25":false,"entitlement-446":true,"pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"12","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":7692006,"Seg12":"ACTIVE","Seg101v":27,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id":"[redacted]","Seg103v":false}}},"prefetch":{"views":[{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:secure:inner-door","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":7692006,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg101v":27,"Seg516e":false,"Seg126v":false,"modval":6,"Seg21":100453,"Seg22":"","Seg24":"urn:kp:prodiem","Seg25":false,"entitlement-446":true,"pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"12","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":7692006,"Seg12":"ACTIVE","Seg101v":27,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id":"[redacted]","Seg103v":false}}]},"telemetry":{"entries":[{"requestId":3198432,"timestamp":1686076871023,"execution":3.6},{"execution

[43] Specific identifier number has been redacted.

":106.5,"parsing":0.2,"request":{"tls":4.2,"timeToFirstByte":88.8,"download":0.7,"responseSize":1534},"telemetryServerToken":"GRgdNPKF2baxcRHAQqAHqyTPswyQefSCMFGH9GY2aUI=","mode":"edge","features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},"requestId":"2499aa7a302a46319e851646fe207f5f","timestamp":1686076871017}]}}

183. As another example, when Plaintiff Jane Doe logged into the Portal on May 31, 2023, the following data was intercepted by Adobe and sent to Adobe's server at the kaiser.tt.omtrdc.net subdomain:

{"requestId":"f33def0d509a49e1beb96b320fcae2fd","context":{"userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36","clientHints":{"mobile":false,"platform":"Windows","browserUAWithMajorVersion":"\"Google Chrome\";v=\"113\", \"Chromium\";v=\"113\", \"Not-A.Brand\";v=\"24\""},"timeOffsetInMinutes":-420,"channel":"web","screen":{"width":1366,"height":768,"orientation":"landscape","colorDepth":24,"pixelRatio":1},"window":{"width":1349,"height":357},"browser":{"host":"healthy.kaiserpermanente.org","webGLRenderer":"ANGLE (Intel, Intel(R) HD Graphics Direct3D11 vs_5_0 ps_5_0, D3D11)"},"address":{"url":"https://healthy.kaiserpermanente.org/consumer-sign-on#/signon","referringUrl":"https://healthy.kaiserpermanente.org/washington/front-door"},"beacon":true},"id":{"tntId":"[redacted]","marketingCloudVisitorId":"[redacted]"},"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"75CDF51005725EB2-38AA41AF056F9156"}},"telemetry":{"entries":[{"requestId":3198432,"timestamp":1685576844326,"execution":312.9},{"execution":540.4,"parsing":1.1,"request":{"tls":30.3,"timeToFirstByte":171,"download":3.5,"responseSize":1323},"telemetryServerToken":"GRgdNPKF2baxcRHAQqAHq1m+lb9PISy9OC4JmXflkxk=","mode":"edge","features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},"requestId":"57f7290ecb644e209d081d8859b9dcb3","timestamp":1685576843853}]},"notifications":[{"id":"5aed303df02141b3a56280a73c83f7b3","type":"display","timestamp":1685576849764,"parameters":{"Seg18v":"","Seg17v":"","Seg55v":"Logged Out","Seg181v":"","Seg81v":"kporg:consumer-sign-on","Seg114vcookie":"","reEnable":"","throttle-area":""},"profileParameters":{"region":"","Seg2":"23"},"view":{"name":"signon"}}],"impressionId":"c1f577b2a5494fd3a0c74f9e6e4ef092"}

184. The first block color coded in blue is sent as part of the HTTP request header and is used to create a digital fingerprint for the specific user by collecting information about the specific user's browser and device information, including details about the user's browser type, computing device, operating system, screen height and width, and details about the user's graphics card. Together these details create a device fingerprint[44] which allows Adobe to compile and track long-

[44] *Fingerprinting*, web.dev, https://web.dev/learn/privacy/fingerprinting/ (last visited Dec. 5, 2024).

term records of the individual's browsing history (and thus deliver targeted advertising or targeted exploits) even when visitors are attempting to avoid tracking—raising a major concern for internet privacy advocates.

185. Web fingerprinting, also known as browser or device fingerprinting, is a process by which companies like Adobe and other Third Party Wiretappers collect and analyze data about browser and system configuration to uniquely identify and track a User's device across the Web. After receiving user data such as browser information (such as browser type, version, active plugins, and language settings), device setting (such as information about the CPU, screen resolution, operating system, and other device details), network settings (such as IP address, Internet service provider, and approximate geographic location), algorithms are then used on the compiled data to create a unique "fingerprint" of the User's device. These fingerprints can be very unique, allowing Websites to identify and track Users and/or their devices over time. This data can also be used to track Users across various devices—known as cross device fingerprinting. For example, when a User logs into an account from both their computer and phone, those separate device fingerprints can now be attached to the User.

186. The second block (green) indicates the URL for the Webpage currently visited by the user. Here, Adobe is receiving information that Plaintiffs logged-into the Portal, signifying that Plaintiffs are Kaiser Plan Members and Kaiser patients—information which Kaiser is prohibited from disclosing under HIPAA and other state and federal laws.

187. The third block (yellow) includes two identifiers set by Adobe: (1) marketingCloudVisitorID and (2) tntID. These identifiers work in tandem with the demdex.net server and the AMCV cookie to help specifically identify users.

188. The above URL headers (and all other URL headers detailed herein) are provided as examples of the type of confidential, personally identifying information, and personal health information that has been intercepted by the Third Party Wiretappers, and similar confidential, personally identifying information, and personal health information, including HIPAA-protected PHI, was transmitted to the Third Party Wiretappers every time Plaintiffs and other Users navigated the Site and Apps.

189. In addition to these URL headers, each time the Adobe code intercepted and redirected Plaintiffs and other Kaiser Plan Members' communications on the Site and Apps, Adobe also received Plaintiffs and other Kaiser Plan Members' IP addresses, which were included in the network traffic sent to Adobe along with the URL header. Although there were ways to prevent Adobe from receiving Plaintiffs and other Kaiser Plan Members' IP addresses, upon information and belief, Kaiser chose not to implement such technology until approximately November 2023 when Kaiser represented to this Court that it had disabled, deleted, or modified the Adobe code on the Site and Apps after the Initial Complaint and Preliminary Injunction Motion were filed.

190. When a user first visits a site with the Adobe Experience Cloud installed, like when Plaintiffs and other Kaiser Plan Members visit the Site and/or Portal, Adobe checks to see if the AMCV cookie is set. This cookie stores the marketingCloudVisitorID (also known as Experience Cloud ID). According to Adobe, the marketingCloudVisitorID "is a universal and persistent ID that identifies your visitors across all solutions in the Experience Cloud."[45] In the POST calls referenced above, the marketingCloudVisitorID for Plaintiffs are assigned specific numeric values (for example, 8[redacted] for Plaintiff Jane Doe and [redacted] for Plaintiff John Doe). This in turn allows for tracking of Kaiser Plan Members across Kaiser sites and across devices as Kaiser's own illustration of its hypothetical patient receiving a flu shot demonstrates.[46].

191. If the AMCV cookie is not set, the Adobe code places a call to the demdex.net server, which generates a marketingCloudVisitorID and sets the AMCV cookie with that value. It also sets a demdex ID cookie which is persistent.[47] Since the marketingCloudVisitorID is stored in the AMCV cookie, it will remain the same for anyone using the browser for that specific site. When a User visits another site with Adobe Experience Cloud installed, a new marketingCloudVisitorID will be generated, but the demdex ID will remain the same. According to Adobe, "[t]he demdex ID remains

[45] *Adobe Target Delivery API (1.0.0) Terms of Service*, Adobe (last updated July 16, 2023), https://experienceleague.adobe.com/en/docs/target-dev/developer/api/delivery-api/identifying-visitors.
[46] *See* ¶ 170 *supra.*
[47] *How the Experience Cloud Identity Service requests and sets IDs*, Adobe (last updated Nov. 10, 2022), https://experienceleague.adobe.com/docs/id-service/using/intro/id-request.html?lang=en.

the same . . . because it's contained in a third party cookie and persists across different domains."[48] This in turn allows Adobe to track specific devices across sites.

192. According to Adobe the tntID, "can be seen as a device ID."[49] As detailed above, device IDs use the unique setup of a user's computer and browser to establish a device fingerprint. This fingerprint can track users across various Websites to build a profile based on their Web browsing habits. In the POST calls referenced above, the tntID is assigned a specific numeric value [redacted] for Plaintiff Jane Doe and [redacted] for Plaintiff John Doe). The tntID is stored in the persistent mbox cookie. Adobe uses the tntID as the main identifier for its Adobe Target solution.[50] The Adobe Target system is used to personalize a user's experience on a website, like Kaiser Plan Members on the Site and Portal. By default, Adobe Target captures the following data, which in turn allows the website to serve personalized and targeted information to specific users:

Data category	Description
Environment parameters	Information about a user's environment, including operating system, browser, and time of day/day of week.
Geography	Information about a user's geography, obtained via IP lookup.
Mobile device	Information about a user's mobile device.
Target reporting segments	Reporting segments configured in Target reporting.
Session behavior	Information about user behavior, such as number of pages viewed.[51]

[48] *Id.*
[49] *Adobe Target Delivery API (1.0.0) Terms of Service*, Adobe (last updated July 16, 2023), https://experienceleague.adobe.com/en/docs/target-dev/developer/api/delivery-api/identifying-visitors .
[50] *Id.*
[51] Adapted from: *Data used by Target machine-learning algorithms*, Adobe (last updated Apr. 23, 2023), https://experienceleague.adobe.com/docs/target/using/activities/automated-personalization/ap-data.html.

193. According to Adobe, the thirdPartyID "is a persistent ID that your business utilizes to identify an end-user regardless of whether they are interacting with your business from web, mobile, or IoT channels. In other words, the thirdPartyId will reference user profile data that can be utilized across channels."[52] In John Doe's POST call referenced above, the thirdPartyId is assigned a specific numeric value ([redacted]). This ID can be used to identify return users once they have logged into the Portal. This in turn allows Adobe's customers to associate the thirdPartyID with a specific individual, the third party here being Kaiser Plan Members.

194. The fourth block (grey) includes customerIds that can be, "added and associated with an Experience Cloud Visitor ID."[53] In the case of the POST call above, the additional data includes the fact the user is authenticated (logged in), again signifying that Plaintiff is a Kaiser Plan Member and Kaiser patient—information which Kaiser is prohibited from disclosing under HIPAA and other state and federal laws and its express and implied contracts with Kaiser Plan Members.

195. These unique identifiers, particularly when combined with other data collected by Adobe such as IP addresses, device fingerprint information, and other data supplied by third party data sources such as [redacted] allows Adobe to identify Plaintiffs and other Kaiser Plan Members and their locations, devices, and online activity so that they can be specifically targeted with ads by Kaiser and other third parties using Adobe's advertising technology.

196. Similar POST calls to kaiser.tt.omtrdc.net are made from other pages on the Site, including main page for the Kaiser Operating States, doctor search, retrieving test results, and the bill pay page.

197. For example, after Plaintiff Jane Doe logged into the Portal and accessed test results on May 31, 2023, Adobe intercepted and received information about the fact Plaintiff Jane Doe had lab test results available (see green highlight), which was transmitted to Adobe and stored on Adobe's kaiser.tt.omtrdc.net server:

{"requestId":"e89a72b9d34c409ebbeec86e8d421e30","context":{"userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

[52] *Adobe Target Delivery API (1.0.0) Terms of Service*, Adobe (last updated July 16, 2023), https://experienceleague.adobe.com/en/docs/target-dev/developer/api/delivery-api/identifying-visitors.

[54] Alphabet, Annual Report (Form 10-K) (Jan. 31, 2024).

Chrome/113.0.0.0
Safari/537.36","clientHints":{"mobile":false,"platform":"Windows","browserUAWithMajorVersion":"\"Google Chrome\";v=\"113\", \"Chromium\";v=\"113\", \"Not-A.Brand\";v=\"24\""},"timeOffsetInMinutes":-420,"channel":"web","screen":{"width":1366,"height":768,"orientation":"landscape","colorDepth":24,"pixelRatio":1},"window":{"width":1349,"height":357},"browser":{"host":"wa-member2.kaiserpermanente.org","webGLRenderer":"ANGLE (Intel, Intel(R) HD Graphics Direct3D11 vs_5_0 ps_5_0, D3D11)"},"address":{"url":"https://wa-member2.kaiserpermanente.org/MyChart/inside.asp?mode=labdetail&eorderid=WP-24dwjwXsqOLR9HkFJIJ-2BBnKA9ug2421MnQJWoSc-2Bc79kw-3D-24kgLeo5NOVUqzvhbO5PbT2bSZ1zLoJ7dRShqNeRddSXk-3D","referringUrl":"https://wa-member2.kaiserpermanente.org/mychart/Clinical/TestResults"}},"id":{"tntId":"[redacted]","thirdPartyId":"[redacted]","marketingCloudVisitorId":"[redacted]","customerIds":[{"id":"[redacted]","integrationCode":"kpaamidepp","authenticatedState":"authenticated","type":"DS"},{"id":"1[redacted]","integrationCode":"kpaamidudr","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"kpaamid_One-off-datasets","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"pzn_crm","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"mbox3rdPartyId","authenticatedState":"authenticated","type":"DS"}]},"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"1926210C0731CEF9-0CC37604F49C1490"}},"execute":{"pageLoad":{"parameters":{"Seg18v":"wa","Seg17v":"wa","Seg55v":"Logged In","Seg181v":"","Seg81v":"","Seg114vcookie":"mbr","reEnable":"","throttle-area":""},"profileParameters":{"region":"","Seg2":"20"}}},"prefetch":{"views":[{"parameters":{"Seg18v":"wa","Seg17v":"wa","Seg55v":"Logged In","Seg181v":"","Seg81v":"","Seg114vcookie":"mbr","reEnable":"","throttle-area":""},"profileParameters":{"region":"","Seg2":"20"}}]},"telemetry":{"entries":[{"requestId":3198432,"timestamp":1685577421980,"execution":194.1},{"execution":226.7,"parsing":0.3,"request":{"tls":27.7,"timeToFirstByte":55.3,"download":6.1,"responseSize":1005},"telemetryServerToken":"GRgdNPKF2baxcRHAQqAHq1m+lb9PISy9OC4JmXflkxk=","mode":"edge","features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},"requestId":"43b0d783fec64ed0a8f15aa346982faa","timestamp":1685577421736}]}
}

198. After Plaintiff John Doe accessed his medical history from within the Portal, Adobe intercepted and received information about the fact Plaintiff John Doe suffers from headaches (see green highlight), which was transmitted to Adobe and stored on Adobe's kaiser.tt.omtrdc.net server:

{"requestId":"8e07062bb9e84eadb2bb393dac657698","context":{"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0
Safari/537.36","clientHints":{"mobile":false,"platform":"macOS","browserUAWithMajorVersion":"\"Google Chrome\";v=\"113\", \"Chromium\";v=\"113\", \"Not-A.Brand\";v=\"24\""},"timeOffsetInMinutes":-420,"channel":"web","screen":{"width":1512,"height":982,"orientation":"landscape","colorDepth":30,"pixelRatio":2},"window":{"width":1512,"height":559},"browser":{"host":"healthy.kaiserpermanente.org","webGLRenderer":"ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)"},"address":{"url":"https://healthy.kaiserpermanente.org/southern-california/secure/search-medical-record?uri=search%3ahealth-

encyclopedia&type=ICD&queryICD10=R51.9&label=HEADACHE&groupName=Health+summary","referringUrl":"https://healthy.kaiserpermanente.org/hconline/ie/inside.asp?lang=english&mode=snapshot"}},"id":{"tntId":"[redacted]","thirdPartyId":"[redacted]","marketingCloudVisitorId":"[redacted]","customerIds":[{"id":"[redacted]","integrationCode":"kpaamidepp","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"kpaamidudr","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"kpaamid_One-off-datasets","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"pzn_crm","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"mbox3rdPartyId","authenticatedState":"authenticated","type":"DS"}]},"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"0E8C61D7B797A752-08C07E6DBCFCCB5A"}},"execute":{"pageLoad":{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:secure:search-medical-record","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":7692006,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg101v":27,"Seg516e":false,"Seg126v":false,"modval":6,"Seg21":100453,"Seg22":"","Seg24":"urn:kp:prodiem","Seg25":false,"entitlement-446":true,"pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"12","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":7692006,"Seg12":"ACTIVE","Seg101v":27,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id":"[redacted]","Seg103v":false}}},"prefetch":{"views":[{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:secure:search-medical-record","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":7692006,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg101v":27,"Seg516e":false,"Seg126v":false,"modval":6,"Seg21":100453,"Seg22":"","Seg24":"urn:kp:prodiem","Seg25":false,"entitlement-446":true,"pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"12","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":7692006,"Seg12":"ACTIVE","Seg101v":27,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id":"[redacted]","Seg103v":false}}]},"telemetry":{"entries":[{"requestId":3198432,"timestamp":1686077690690,"execution":12.7},{"execution":120.9,"parsing":0.1,"request":{"tls":1.8,"timeToFirstByte":93.3,"download":0.8,"responseSize":1658},"telemetryServerToken":"GRgdNPKF2baxcRHAQqAHqyTPswyQefSCMFGH9GY2aUI=","mode":"edge","features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},"requestId":"30377aef3045436aa832ba402fe7c5ca","timestamp":1686077690672}]}}

199. Similarly, after Plaintiff John Doe accessed his medical history from within the Portal, Adobe intercepted and received information about the fact that Plaintiff John Doe suffers from kidney stones (see green highlight), which was transmitted to Adobe and stored on Adobe's kaiser.tt.omtrdc.net server:

{"requestId":"c7c2f6533c974a37bf18df244b7860ac","context":{"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/113.0.0.0
Safari/537.36","clientHints":{"mobile":false,"platform":"macOS","browserUAWithMajorVersion":"\"Google Chrome\";v=\"113\", \"Chromium\";v=\"113\", \"Not-A.Brand\";v=\"24\""},"timeOffsetInMinutes":-420,"channel":"web","screen":{"width":1512,"height":982,"orientation":"landscape","colorDepth":30,"pixelRatio":2},"window":{"width":1512,"height":732},"browser":{"host":"healthy.kaiserpermanente.org","webGLRenderer":"ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)"},"address":{"url":"https://healthy.kaiserpermanente.org/southern-california/pages/search?query=kidney+stones&category=global&global-region=sca&language=english&region=sca","referringUrl":"https://healthy.kaiserpermanente.org/southern-california/front-door"}},"id":{"tntId":"[redacted]","marketingCloudVisitorId":"45551410577000512211724311790756648518"},"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"RKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"1385A481D134AE9C-5442EE55E30D9036"}},"execute":{"pageLoad":{"parameters":{"Seg18v":"sca","Seg17v":"","Seg55v":"Logged Out","Seg181v":"","Seg81v":"kporg:pages:search","Seg114vcookie":"","reEnable":"","throttle-area":""},"profileParameters":{"region":"","Seg2":"12"}}},"prefetch":{"views":[{"parameters":{"Seg18v":"sca","Seg17v":"","Seg55v":"Logged Out","Seg181v":"","Seg81v":"kporg:pages:search","Seg114vcookie":"","reEnable":"","throttle-area":""},"profileParameters":{"region":"","Seg2":"12"}}]},"telemetry":{"entries":[{"requestId":3198432,"timestamp":1686079858947,"execution":31},{"execution":347.9,"parsing":0.1,"request":{"tls":1.4,"timeToFirstByte":301.7,"download":0.3,"responseSize":3542},"telemetryServerToken":"13OD8mmKQLOFlv9DVqEli/66cI/n43cYFW7Bbdgc7oQ=","mode":"edge","features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},"requestId":"d1ee96fe7bc44f32a598fa3fa6301fec","timestamp":1686079858912}]}}

200. In another example, when Plaintiff John Doe accessed his medications from within the Portal, Adobe intercepted and received information about the fact that Plaintiff John Doe takes a certain medication (see green highlight), which was transmitted to Adobe and stored on Adobe's kaiser.tt.omtrdc.net server:

{"requestId":"4b353a7157fe4afb994b10217d877637","context":{"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0
Safari/537.36","clientHints":{"mobile":false,"platform":"macOS","browserUAWithMajorVersion":"\"Google Chrome\";v=\"113\", \"Chromium\";v=\"113\", \"Not-A.Brand\";v=\"24\""},"timeOffsetInMinutes":-420,"channel":"web","screen":{"width":1512,"height":982,"orientation":"landscape","colorDepth":30,"pixelRatio":2},"window":{"width":1512,"height":559},"browser":{"host":"healthy.kaiserpermanente.org","webGLRenderer":"ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)"},"address":{"url":"https://healthy.kaiserpermanente.org/southern-california/health-wellness/drug-encyclopedia/drug.259872","referringUrl":"https://healthy.kaiserpermanente.org/hconline/ie/inside.asp?lang=english&mode=snapshot"}},"id":{"tntId":"[redacted]","thirdPartyId":"[redacted]","marketingCloudVisitorId":"[redacted]","customerIds":[{"id":"1[redacted]","integrationCode":"kpaamidepp","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":

"kpaamidudr","authenticatedState":"authenticated","type":"DS"},{"id":"1[redacted]","integrationCode":"kpaamid_One-off-datasets","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"pzn_crm","authenticatedState":"authenticated","type":"DS"},{"id":"[redacted]","integrationCode":"mbox3rdPartyId","authenticatedState":"authenticated","type":"DS"}]},"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"1EE577E8629305D2-08A3CF719904939A"}},"execute":{"pageLoad":{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:health-wellness:drug-encyclopedia:drug.259872","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":7692006,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg101v":27,"Seg516e":false,"Seg126v":false,"modval":6,"Seg21":100453,"Seg22":"","Seg24":false,"Seg25":false,"entitlement-446":"","entity.id":"%monograph_id%","pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"12","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":7692006,"Seg12":"ACTIVE","Seg101v":27,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id":"[redacted]","Seg103v":false}}},"prefetch":{"views":[{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:health-wellness:drug-encyclopedia:drug.259872","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":7692006,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg101v":27,"Seg516e":false,"Seg126v":false,"modval":6,"Seg21":100453,"Seg22":"","Seg24":false,"Seg25":false,"entitlement-446":"","entity.id":"%monograph_id%","pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"12","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":7692006,"Seg12":"ACTIVE","Seg101v":27,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id":"[redacted]","Seg103v":false}}]},"telemetry":{"entries":[{"requestId":3198432,"timestamp":1686077727535,"execution":13.1},{"execution":536,"parsing":0.1,"request":{"tls":29.6,"timeToFirstByte":453.5,"download":9,"responseSize":1652},"telemetryServerToken":"ytSZo63c32LTWU3OagsNm4f2oPeqNn97fefLHdLznd4=","mode":"edge","features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},"requestId":"de495a765e94495db656689de5179016","timestamp":1686077727519}]}}

201. When Plaintiff Jane Doe logged out of the Portal and conducted a search for a doctor using the keyword "mental health" on the Site, the POST to kaiser.tt.omtrdc.net revealed the search term as shown below (green highlight):

{"requestId":"f42ffe0b90c141e6836a7006c18a6965","context":{"userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36","clientHints":{"mobile":false,"platform":"Windows","browserUAWithMajorVersion":"\"Google Chrome\";v=\"113\", \"Chromium\";v=\"113\", \"Not-A.Brand\";v=\"24\""},"timeOffsetInMinutes":-420,"channel":"web","screen":{"width":1366,"height":768,"orientation":"landscape","colorDepth":24,"pixelRatio":1},"window":{"width":1349,"height":584},"browser":{"host":"healthy.kaiserpermanente.org","webGLRenderer":"ANGLE (Intel, Intel(R) HD Graphics Direct3D11 vs_5_0 ps_5_0,

D3D11)"},"address":{"url":"https://healthy.kaiserpermanente.org/washington/doctors-locations#/facility-results?zipcode=98203&keyword=mental%20health","referringUrl":"https://healthy.kaiserpermanente.org/doctors-locations"},"beacon":true},"id":{"tntId":[redacted],"marketingCloudVisitorId":"[redacted]"},"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"RKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"16848F6EF92A646D-091DAB5A2A2A31A4"}},"notifications":[{"id":"1251619415694631 9b158793ad9744d1","type":"display","timestamp":1685579001396,"parameters":{"Seg18v":"wa","Seg17v":"","Seg55v":"Logged Out","Seg181v":"","Seg81v":"kporg:doctors-locations","Seg114vcookie":"","reEnable":"","throttle-area":""},"profileParameters":{"region":"","Seg2":"23"},"view":{"name":"facility-results"}}],"impressionId":"2017e8f257b548dbb2e29e2e51bcdc38"}

202. Similarly, when Plaintiff John Doe logged out of the Portal and conducted a search for a neurologist on the Site, the POST to kaiser.tt.omtrdc.net revealed the search term and Plaintiff's zip code as shown below (green highlight):

{"requestId":"c059ddb0f7ee4602ad5c1cf0e72e6e0f","context":{"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36","clientHints":{"mobile":false,"platform":"macOS","browserUAWithMajorVersion":"\"Google Chrome\";v=\"113\", \"Chromium\";v=\"113\", \"Not-A.Brand\";v=\"24\""},"timeOffsetInMinutes":-420,"channel":"web","screen":{"width":1512,"height":982,"orientation":"landscape","colorDepth":30,"pixelRatio":2},"window":{"width":1512,"height":769},"browser":{"host":"healthy.kaiserpermanente.org","webGLRenderer":"ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)"},"address":{"url":"https://healthy.kaiserpermanente.org/southern-california/doctors-locations#/providers?zipcode=92395&medical_specialty_label=Psychiatry%20%26%20Neurology:%20Neurology,Psychiatry%20%26%20Neurology:%20Psychiatry","referringUrl":"https://healthy.kaiserpermanente.org/southern-california/doctors-locations"}},"id":{"tntId":"[redacted]","marketingCloudVisitorId":"45551410577000512211724311790756648518"},"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"RKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"2B0396D39B44DC65-28244F36559B11C5"}},"execute":{"pageLoad":{"parameters":{"Seg18v":"sca","Seg17v":"","Seg55v":"Logged Out","Seg181v":"","Seg81v":"kporg:doctors-locations","Seg114vcookie":"","reEnable":"","throttle-area":"","providerType":"","keyword":"","specialty":"Psychiatry & Neurology: Neurology,Psychiatry & Neurology: Psychiatry","healthPlan":""},"profileParameters":{"region":"","Seg2":"12"}}},"prefetch":{"views":[{"parameters":{"Seg18v":"sca","Seg17v":"","Seg55v":"Logged Out","Seg181v":"","Seg81v":"kporg:doctors-locations","Seg114vcookie":"","reEnable":"","throttle-area":"","providerType":"","keyword":"","specialty":"Psychiatry & Neurology: Neurology,Psychiatry & Neurology: Psychiatry","healthPlan":""},"profileParameters":{"region":"","Seg2":"12"}}]}}

203. When Plaintiffs John Doe II, John Doe III, Jane Doe II, Jane Doe III, Jane Doe IV, Jane Doe V, and Alexis Sutter accessed the Kaiser website and Patient Portal, their communications were similarly intercepted by Adobe.

204. On information and belief, the same type of information tracked, disclosed, and sent to Adobe for Plaintiffs has been tracked, disclosed, and sent to Adobe for other members of the Classes.

205. Kaiser purposefully collected Plaintiffs' and Class Members' personally identifiable information while also installing Adobe's code on its website and mobile applications and failing to prevent and/or aiding and abetting in that personally identifiable information being intercepted by Adobe thereby compromising Plaintiffs' and Class Members' privacy and the confidentiality of their personally identifiable information. Thus, by allowing Adobe to intercept Kaiser Plan Members' information and communications from the Site and Apps, Kaiser foreseeably harmed Plaintiffs and similarly situated Class Members.

206. Defendants knew or should have known that they were failing to comply with the applicable statutes and common law duties governing their conduct, and that Defendants' breach would cause Plaintiffs and Class Members to experience foreseeable harms associated with the unauthorized interception, disclosure, and use of their personal health information by Adobe.

3. Kaiser Allows Twitter, Microsoft Bing, and/or Google to Intercept Users' Communications from the Site and Apps

207. Kaiser, on its Home Page, Portal Login Page, and other pages on the Site—including within the Portal—and Apps also uses code that sends confidential and protected health information to Twitter, Microsoft Bing, and/or Google.

208. The Microsoft Bing, Google, and Twitter code sends data to their respective servers via HTTP GET and/or the POST request parameters.

209. Unlike the POST request described above, the HTTP GET method requests data from a server. This request can include additional parameters that are sent as part of the request URL. For example, take the request "www.example.com ?utm_source=google." In this case, everything after

the "?" is used to track additional data, such as where the site visitor came from, in this case showing that the visitor came from Google before accessing the www.example.com.

210. In addition to these URL headers, each time the Twitter, Microsoft Bing, or Google code intercepted and redirected Plaintiffs and other Kaiser Plan Members' communications on the Site and Apps, Twitter, Microsoft Bing, and Google also received Plaintiffs' and other Kaiser Plan Members' IP addresses, which were included in the network traffic sent to Twitter, Microsoft Bing and Google along with the URL header.

211. Although there were ways to prevent Twitter, Microsoft Bing, and Google from receiving Plaintiffs and other Kaiser Plan Members' IP addresses, upon information and belief, Kaiser failed to implement such technology until approximately November 2023 when Kaiser represented to this Court that it had disabled, deleted, or modified the Twitter, Microsoft Bing, and Google code on the Site and Apps after the Initial Complaint and Preliminary Injunction Motion were filed.

212. In fact, as Kaiser acknowledged in its recent disclosures to state and federal regulators, these online technologies provided by Google, Microsoft Bing, and Twitter, collected HIPAA-protected PHI from Kaiser Health Plan Members, which until November 2023 included, *inter alia*, Kaiser Health Plan Members' IP addresses, names, information that could indicate a member was signed into a Kaiser account or service, information showing how the member interacted with and navigated through the website or mobile applications, and search terms used in the health encyclopedia.

213. Google and Microsoft Bing are the most widely used search engines, and Twitter is one of the largest social media sites in the world. Generally, Google, Microsoft Bing, and Twitter do not charge to use their services because they are able to generate billions of dollars in revenue each year by selling targeted advertising.

214. A main goal for Google, Microsoft Bing, and Twitter is to develop a profile of users to better target them with ads. These advertising networks are significant to each of these entities. For example, the Google Network has its own revenues separately reported in Alphabet (Google's parent company) Form 10-K (annual report to the SEC and shareholders). For the 2023 fiscal year, Alphabet

reported over $31 billion in revenue attributable to the Google Network.[54] As described by Google, "The Google Network can connect you with customers at the exact moment when they're doing an activity online that relates to what you offer -- like searching for your product or reading a blog about your industry. Because your ads can be shown in relevant places, you have a better chance of turning viewers into customers."[55] Connecting advertisers "at the exact moment when they're doing an activity online" requires an incredible ingestion of data through products such as the "free" technology used by Kaiser.[56] Therefore, all these sites offer "free" analytics technology to companies like Kaiser.

215. In exchange for this "free" technology to get information about who is visiting Kaiser's Site and Apps, Kaiser provided these companies access to Kaiser Plan Members and their data. With this information, Google, Bing, and Twitter were able to expand their advertising networks in terms of data tied to the unique profiles for users and also in terms of overall size. This information is highly valuable and necessary to support their advertising networks. This technology is useful to advertisers as they can show how effective certain ads are. Web analytics technology also provide general information about who is visiting the website and what those users are doing on the site.

216. [redacted]

217. However, part of the implicit cost of this Google, Microsoft Bing, and Twitter technology is the ability to allow Google, Microsoft Bing, and Twitter to use the information received

[54] Alphabet, Annual Report (Form 10-K) (Jan. 31, 2024).

[55] The Google Network, Google, https://support.google.com/google-ads/answer/1721923?sjid=16879293567354684444-NA (last visited Dec. 5, 2024).

[56] Similarly, Microsoft Bing is part of Microsoft's Search and news advertising segment, which reported over $12.2 billion in revenue for fiscal year 2023 according to Microsoft Inc. Form 10-K for the 2023 Fiscal Year filed with the SEC on July 27, 2023. Twitter is owned by X Corp., a private company and does not report its revenues.

to supplement user profiles for better targeting and bolster their ad networks. Kaiser thus understood that, in lieu of monetary payments for the use of the Google, Microsoft Bing, and Twitter code, Kaiser would be paying Google, Microsoft Bing, and Twitter in kind by providing them with personally identifying information and PHI from Kaiser Health Plan members that Google, Microsoft Bing, and Twitter could then monetize.

218. Kaiser acted willfully and deceptively by engaging in the unauthorized interception, disclosure, and transfer of private health information to Google, Microsoft Bing, and Twitter for their own and other third parties' use in violation of its own Site Terms and Conditions so that Kaiser could obtain "free" use of Google, Microsoft Bing, and Twitter's products.

a) Twitter Uses Kaiser Plan Members' Personally Identifying Information and PHI from the Site and Kaiser Permanente App for its Own and Other Third Parties' Marketing

219. Twitter collects a vast array of information about the public so that it can be used to develop profiles and better target specific individuals with ads.

220. For example, if a user tweets about a current event in the news or about their job, Twitter and advertisers can understand a user's political leanings or job type. This information is valuable to Twitter because it helps advertisers understand who Twitter users are so that Twitter can sell advertisements targeting that particular user's Twitter timelines.[57]

221. Twitter also tracks browsing activity outside of Twitter, for both Twitter users and people who have never created an account on the Twitter platform, including browser type, the device and operating system, the mobile carrier, IP address, and browsing activity.[58] Twitter can also learn information about websites visited before landing on the referring website and what websites were visited after leaving the site.[59]

222. As particularly relevant here, Twitter also tracks user information provided by ad partners, such as Kaiser, that embed code on their website and in the mobile applications.

[57] Mehak Siddiqui, *What Does Twitter Know About Me?*, vpnoverview (Sept. 9, 2022), https://vpnoverview.com/privacy/social-media/what-does-twitter-know-about-me/.
[58] *Id.*
[59] *Id.*

223. As explained in Twitter's Privacy Policy, personally identifiable information received from partners such as Kaiser is combined with other data collected by Twitter to develop user profiles to better target ads:

> Ad Partners, Developers, Publishers.
>
> Our ad and business partners share information with us such as browser cookie IDs, X-generated identifiers, mobile device IDs, hashed user information like email addresses, demographic or interest data, and content viewed or actions taken on a website or app. Some of our ad partners, particularly our advertisers, also enable us to collect similar information directly from their website or app by integrating our advertising technology. **Information shared by ad partners and affiliates or collected by X from the websites and apps of ad partners and affiliates may be combined with the other information you share with X and that X receives, generates, or infers about you described elsewhere in this Privacy Policy**.[60]

224. Twitter summarizes how partners, such as Kaiser, can use its analytic technology for marketing. These technologies "are powered by the X website tag, a snippet of code that you place on pages of your website. Once placed, the website tag begins to collect the cookie IDs of visitors ***and matches them to X users***. Once an audience has been created, you can target X Ads campaigns to those recent website visitors."[61] This process "allow[s] you to leverage your off-platform customer information to create unique audience segments that can be used for targeting, exclusion, and lookalike expansion."[62]

225. By embedding Twitter's code on Kaiser's Site and the Kaiser Permanente App, Kaiser was thus aware the Twitter was combining that information about Kaiser Health Plan Members, including their PHI, with other data sources to better enable targeted marketing by Kaiser, Twitter and other third parties using Twitter's technology; indeed, Kaiser installed Twitter's code on its Site and Kaiser Permanente App to access Twitter's marketing capabilities and ability to target specific individuals with relevant content based on their online behavior, including Plaintiffs and other Kaiser Plan Members.

226. Although Twitter received PHI through code embedded on the Site and the Kaiser Permanente App, Kaiser had no contracts with Twitter restraining Twitter's ability to use this

---

[60] *X Privacy Policy*, Twitter (effective Sept. 29, 2023), https://twitter.com/en/privacy.
[61] *See Website Activity Custom Audiences*, Twitter, https://business.twitter.com/en/help/campaign-setup/campaign-targeting/custom-audiences/website-activity.html (last visited Dec. 5, 2024) (emphasis added).
[62] *Intro to Custom Audiences*, Twitter, https://business.x.com/en/help/campaign-setup/campaign-targeting/custom-audiences.html (last visited Dec. 5, 2024).

information for Twitter's own or other third parties' advertising purposes, nor did Kaiser enter into a Business Associate Agreement with Twitter. To the contrary, Twitter's privacy policy explicitly ***allows*** Twitter to use this data for its own purposes, including marketing.[63] Kaiser had no contracts with Twitter prohibiting it from using Kaiser Plan Members' confidential information, including PHI, for its own or other third parties' purposes as recognized in the Twitter Privacy Policy.

227. Nonetheless, Kaiser knowingly allowed Twitter to intercept Plaintiffs' and other Kaiser Plan Members' PHI from the time Kaiser installed Twitter's code on its Site and the Kaiser Permanente App until approximately November 2023 when Kaiser represented to this Court that it had disabled, deleted, or modified the Twitter code on the Site and Apps after the initial Complaint, First Amended Complaint, and Preliminary Injunction Motion were filed.

228. By way of example, when Plaintiff Jane Doe accessed the Portal, Twitter sent two GET requests—one to analytics.twitter.com and one to t.co. Except for the base domain, both GET requests were the same as follows:

> https://analytics.twitter.com/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=5f8ad0cc-d7e4-4c79-be40-b2476d38e9c6&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=751184a7-0132-46b9-80db-fa67ceecceec&tw_document_href=https%3A%2F%2Fwa-member.kaiserpermanente.org%2Fhome%2F&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

229. When Plaintiff John Doe accessed the Portal, Twitter sent two GET requests—one to analytics.twitter.com and one to t.co. Except for the base domain, both GET requests were the same as follows:

> https://t.co/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=23676916-ed52-496b-be38-e9067f36cf37&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=eb369f6b-bab7-443a-abfd-6a18f78ec1e2&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

230. As reflected above, highlighted in blue, the Twitter GET requests were used to indicate a page view of a Kaiser Member successfully logging into the Portal.

[63] *See X Privacy Policy*, Twitter (Sept. 29, 2023), https://twitter.com/en/privacy.

231. On June 6, 2023, when Plaintiff John Doe requested an electronic copy of his medical records from inside the Portal, Twitter (both analytics.twitter.com and t.co) received the following information through a GET request:

> https://t.co/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=305bd815-e13e-4eae-ab1e-0fd5d4dfea93&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=85138e85-2f71-4efc-ae39-6cb490e93e87&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DICD%26queryICD10%3DR51.9%26label%3DHEADACHE%26groupName%3DHealth%2Bsummary&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29
>
> https://t.co/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=bdd9fe2d-11a0-4c14-9ea9-075f29bd4fe4&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=3e2ebf5e-3ab3-4c45-8573-df51ad40350a&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fpages%2Fsearch%3Fquery%3Dkidney%2Bstones%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

232. The Twitter GET requests reveal in the current site URL (highlighted in blue) that Plaintiff John Doe suffers from headaches (first GET above) and kidney stones (second GET above). This data can be used to better target ads, in this case showing, for example, headaches so that Plaintiff John Doe could be targeted for such things as pain medication.

233. Alongside these GET requests were specific identifiers from cookies on John Doe's device that identified the information received as pertaining specifically to him so that it could be matched to his advertising profile as maintained by Twitter:

> guest_id_marketing=[redacted];
> guest_id_ads=[redacted]
> personalization_id="[redacted]
> guest_id=[redacted]

234. As described by Twitter, the "personalization_id" cookie "tracks activities on and off Twitter for a personalized experience."[64] Similarly, the "guest_id_marketing" and "guest_id_ads" cookies are "for advertising when logged out [of Twitter]."[65] The "guest_id" cookie "is for authentication."[66]

---

[64] *How cookies are used on X*, Twitter, https://help.twitter.com/en/rules-and-policies/x-cookies (last visited Dec. 5, 2024).
[65] *Id.*
[66] *Id.*

235. On June 6, 2023, when John Doe accessed the medications page from within the Portal, Twitter (both analytics.twitter.com and t.co) received the following information through a GET request:

> https://t.co/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=b343cdf0-a3db-4b81-b74c-34a88cc9960f&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=8ce3fde0-7770-42d2-a833-f63cc049e2f5&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-wellness%2Fdrug-encyclopedia%2Fdrug.259872&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

236. The Twitter GET request includes the current URL (blue) which includes the drug encyclopedia link for the drug 259872 which is Omeprazole 20mg delayed release.

237. Alongside this GET request were the same specific identifiers from cookies on John Doe's device that identified the information received as pertaining specifically to him so that it could be matched to his advertising profile as maintained by Twitter:

> guest_id_marketing=[redacted]
> guest_id_ads=[redacted]
> personalization_id=[redacted]
> guest_id=[redacted]

238. When Plaintiff Jane Doe conducted a search for "mental health" on the Site, Twitter (both analytics.twitter.com and t.co) received the following information through a GET request:

> https://analytics.twitter.com/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=40e2b65d-4a2e-4272-a887-d0a74c97457c&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=bea70ac7-252c-4537-9a9d-754bd29d7111&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

239. The Twitter GET request in the current site URL (highlighted in blue) reveals that Plaintiff Jane Doe searched on the term "mental health." This data can similarly be used to better target ads.

240. Each time Plaintiffs John Doe II, John Doe III, Jane Doe II, Jane Doe III, Jane Doe IV, Jane Doe V, and Alexis Sutter accessed the Kaiser Site, including the Patient Portal, and Kaiser Permanente App their communications were similarly intercepted by Twitter.

241. For example, when Plaintiff Jane Doe IV was logged into the Portal on September 12, 2023 and tried to schedule an appointment, Twitter (both analytics.twitter.com and t.co) received the following information through a GET request:

> https://analytics.twitter.com/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=7672294d-f821-4294-bf0a-7ff7d29b3a8f&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=500a1ab2-cbe6-4923-9bd0-9aa90379fadd&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fmaryland-virginia-washington-dc%2Fsecure%2Fappointments&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

242. The Twitter GET request in the current site URL (highlighted in blue) reveals that Plaintiff Jane Doe IV was seeking a medical appointment with Kaiser. This data can similarly be used to better target ads. Indeed, the same marketing cookie identifiers, though with different values specific to Jane Doe IV were sent to Twitter:

> guest_id_marketing=[redacted]
> guest_id_ads[redacted]
> personalization_id="[redacted]
> guest_id[redacted]

243. On information and belief, the same type of information tracked, disclosed, and sent to Twitter for Plaintiffs has been tracked, disclosed, and sent to Twitter for all Plaintiffs and other members of the Classes each time they used the Site, including inside the Portal, and the Kaiser Permanente App.

244. Whenever Kaiser Plan Members used Kaiser's Site, Kaiser allows Twitter to intercept the contents of their communications—including personal information, identifying information, and sensitive medical information—without their knowledge, consent, or authorization.

245. Kaiser knowingly redirected and disclosed Kaiser Plan Members' personally identifiable patient information, including their status as patients and the contents of their communications with Kaiser to Twitter.

246. Despite its legal obligations to keep this information and these communications private and confidential, Kaiser's use of Twitter code caused the redirection, interception, and transmission of the precise content of patients' communication with Kaiser to Twitter.

247. Kaiser's unauthorized redirection and disclosures to Twitter includes information that identifies Plaintiffs and Class Members as patients of Kaiser Permanente, and intercepts and/or aids in receiving and recording patient communications pertaining to or about specific medical conditions, health services, and other PHI.

248. Kaiser's disclosures to Twitter occurred because Kaiser intentionally deploys Twitter code on its website, and that code "bugs" Kaiser Plan Members' web-browsers and causes personally identifiable patient information, as well as the contents of communications exchanged between Kaiser and its patients, to be redirected and sent to Twitter.

249. As deployed, Twitter code, as employed by Kaiser, functioned as a wiretap, Twitter as a third party wiretapper.

250. Kaiser purposefully collected Plaintiffs' and Class Members' personally identifiable information while also installing Twitter's code on its website and mobile applications and failing to prevent and/or aiding and abetting in that personally identifiable information being intercepted by Twitter thereby compromising Plaintiffs' and Class Members' privacy and the confidentiality of their personally identifiable information. Thus, by allowing Twitter to intercept Kaiser Plan Members' information and communications from the Site and Apps, Kaiser foreseeably harmed Plaintiffs and similarly situated Class Members.

251. Defendants knew or should have known that they were failing to comply with the applicable statutes and common law duties governing their conduct, and that Defendants' breach would cause Plaintiffs and Class Members to experience foreseeable harms associated with the unauthorized interception, disclosure, and use of their personal health information by Twitter.

b) Google Uses Kaiser Plan Members' Personally Identifying Information and PHI for its Own and Other Third Parties' Marketing

252. Google also collects a vast array of information about Users of the Site and App so that it can be used to develop profiles and better target specific individuals with ads.

253. For example, Google sells ads based on a User's search. So, if a Kaiser Plan Member searches for a medical condition such as cancer, that Kaiser Plan Member can thereafter be targeted with ads for cancer treatment centers.

254. Google is also a widely used ad platform that provides ad remarketing. Remarketing shows ads based on sites a user has previously visited. For example, a user who visits a website with Google code, and searches on pregnancy related topics, might then see ads for a Google advertiser's pregnancy related services on other websites.

255. Historically, Google (and Google's ad-servicing division DoubleClick)[67] largely tracked user behavior was through the use of third party cookies. Unlike a first-party cookie, which allows the website you are visiting to remember details about you like your username and authentical data for when you return to that website, Google has historically used third party cookies that enabled it to track your behavior across multiple websites. Because Google cookies are ubiquitous across the internet, Google can then piece together your interests and proclivities and allow competitors to advertise against each other and purchase the right to target you with their particular ads based on your interests.

256. Because the same cookies are not automatically set on every device you own, and in some instances can be blocked, disabled and/or cleared, Google in or around 2013 announced plans to start assigning an "advertising ID," which makes blocking third party cookies less effective and allows individuals to be tracked more effectively, particularly across different devices and locations.[68]

257. Google also tracks users with their IP addresses. As Google discloses in its policies for partner sites:[69]

> For example, when you visit a website that uses advertising services like AdSense, including analytics tools like Google Analytics, or embeds video content from YouTube, your web browser automatically sends certain information to Google. **This includes the URL of the page you're visiting and your IP address**. We may also set cookies on your browser or read cookies that are already there. Apps that use Google advertising services also share information with Google, such as the name of the app and a unique identifier for advertising.
>
> **Google uses the information shared by sites and apps** to deliver our services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalize content and ads you see on Google and on our partners' sites and apps.

[67] Google acquired DoubleClick in 2008, which Google later merged into its new Google Marketing Platform brand which unified DoubleClick's advertising services and Google's own advertising and analytics services.

[68] David Auerback, *C is for Cookie*, Slate (Sept. 24, 2023 11:52 pm), https://slate.com/technology/2013/09/how-google-uses-cookies-its-so-much-more-complicated-than-we-think.html.

[69] *Privacy & Terms*, Google, https://policies.google.com/technologies/partner-sites (last visited Dec. 5, 2024) (emphasis added).

258. More recently, in or around 2022, Google announced that it would be replacing third party cookie tracking technology "Topics." With Topics,

> [W]hen a user visits a website and the website wants to show an ad, the website can run JavaScript code (or check the request header Sec-Browsing-Topics) to fetch a list of up to three topics, from a taxonomy of several hundred interest categories, derived from the user's past website visits. That allows the site to show an ad believed to be relevant to the visitor's known interests.[70]

259. That list of topics is derived from information Google uses to determine your top interests that week, which remain stored for three weeks and old interests are replaced. Although Google has portrayed Topics as a privacy improvement over its use of third party cookies, Google's announcement was almost immediately met with criticisms and concerns that specific individuals' interests and proclivities could still be identified through device fingerprinting and other techniques.[71]

260. Google also specifically allows advertisers to target individuals with specific health conditions, including multiple highly specific health conditions among the "verticals" or "categories" that can be used to target specific individuals with Google ads, as sampling of which is below:

[70] Thomas Claburn, *Google asks websites to kindly not break its shiny new targeted-advertising API*, The Register (June 27, 2023), https://www.theregister.com/2023/06/27/google_tweaks_topics_api_ahead/.

[71] *Id.* (citing Fingerprinting Threat Using the Topics API Github (May 30, 2022), https://github.com/patcg-individual-drafts/topics/issues/74).

419	45	/Health/Health Conditions
625	419	/Health/Health Conditions/AIDS & HIV
626	419	/Health/Health Conditions/Allergies
628	419	/Health/Health Conditions/Arthritis
630	419	/Health/Health Conditions/Blood Sugar & Diabetes
429	419	/Health/Health Conditions/Cancer
629	419	/Health/Health Conditions/Cold & Flu
1211	419	/Health/Health Conditions/Ear Nose & Throat
571	419	/Health/Health Conditions/Eating Disorders
1328	419	/Health/Health Conditions/Endocrine Conditions
1329	1328	/Health/Health Conditions/Endocrine Conditions/Thyroid Conditions
638	419	/Health/Health Conditions/GERD & Digestive Disorders
941	419	/Health/Health Conditions/Genetic Disorders
559	419	/Health/Health Conditions/Heart & Hypertension
643	559	/Health/Health Conditions/Heart & Hypertension/Cholesterol Issues
632	419	/Health/Health Conditions/Infectious Diseases
1262	632	/Health/Health Conditions/Infectious Diseases/Parasites & Parasitic Diseases
1263	632	/Health/Health Conditions/Infectious Diseases/Vaccines & Immunizations
817	419	/Health/Health Conditions/Injury
942	419	/Health/Health Conditions/Neurological Conditions
641	942	/Health/Health Conditions/Neurological Conditions/Learning & Developmental Disabilities
642	641	/Health/Health Conditions/Neurological Conditions/Learning & Developmental Disabilities/ADD & ADHD
1856	641	/Health/Health Conditions/Neurological Conditions/Learning & Developmental Disabilities/Autism Spectrum Disorders

261. In fact, the threats to privacy posed by Google, and other Third Party Wiretappers' embedded code are so great that the U.S. Department of Health and Human Services, Office for Civil Rights, drafted a letter in July 2023 (attached hereto as Exhibit 7), explaining:

> Recent research, news reports, FTC enforcement actions, and an OCR bulletin have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users.
>
> Impermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others.

> This letter further reinforced that "[i]f you are a covered entity or business associate ('regulated entities') under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium" and that "[t]he HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (e.g., tracking technology vendors) includes PHI."

262. The Kaiser Site and Apps, including inside the Portal, track views via integration with Google code, including Google Analytics, Doubleclick (which as noted above is owned by Google and allows companies pay for clicks and track ad effectiveness) and other Google code and allow Google to use Plaintiffs' and other Kaiser Plan Members' personally identifying information and PHI for targeted advertising.

263. Kaiser was aware of this when it installed the code on its Site and Apps; indeed, Kaiser installed the Google code on its Site and Apps to access Google's marketing capabilities and ability to target specific individuals, including Plaintiffs and other members of the Classes with relevant content based on their online behavior.

264. Kaiser did not have contracts with Google that restricted Google's ability to use Kaiser Plan Members' confidential information and PHI collected with this code for Google's own or other third parties' advertising purposes.

265. For example, in July 2019, Kaiser and Google entered into a Google Cloud Master Agreement, which covered "Google Maps Core Services," which under the "Data use and Retention" section, explicitly allowed Google to use and retain Kaiser Plan Members' personally identifying information, providing:

> Data Use and Retention: To provide the Services through the customer Application(s), Google collects and receives data from Customer and End Users (and End Users' End Users, if any), including search terms, IP addresses, and latitude/longitude coordinates. Customer acknowledges and agrees that Google and its Affiliates may use and retain this data to provide and improve google products and services, subject to the then-current Google Privacy Policy.

Although Kaiser now admits that it provided Google with Kaiser Plan Members' HIPAA-protected PHI through Google Maps and other Google products, Kaiser never entered into any relevant Business Associate Agreements with Google, nor did Kaiser enter into contracts ensuring that Google would not use that information for its own or other third parties' advertising purposes.

266. Moreover, although Google represented to Plaintiffs in February 14, 2024 "that data from KaiserPermanente.org is not used to personalize ads in Google Search, YouTube and Google Display Network," despite repeated requests, Google has failed to confirm ***when*** that restriction applied to the Apps or data received from Kaiser through other means, such as through a connection to Kaiser's Adobe products or through use of Google's Customer Match services. Indeed, based on Kaiser's representations that it disabled, deleted, or modified Google's code in November 2023, it is not surprising that this restriction was in place as of February 14, 2024.

267. Moreover, although Google has also represented that "[g]enerally, healthcare provider websites are classified as sensitive, and data for those websites are not used for personal advertising," "[i]nsurance company websites and apps are generally ***not classified as sensitive***, and data from those websites ***may be used*** for personal advertising." According to Google, as of February 14, 2024, [redacted] while some parts are considered sensitive, others are not." Similarly, despite repeated requests, Google has failed to confirm ***when*** that restriction was put in place, whether that restriction applied to the Apps.

268. Nonetheless, Kaiser knowingly allowed Google to intercept Plaintiffs' and other Kaiser Plan Members' personally identifying information and PHI from the time Kaiser installed Google's code on its Site and Apps until approximately November 2023 when Kaiser represented to this Court that it had disabled, deleted, or modified the Google code on the Site and Apps.

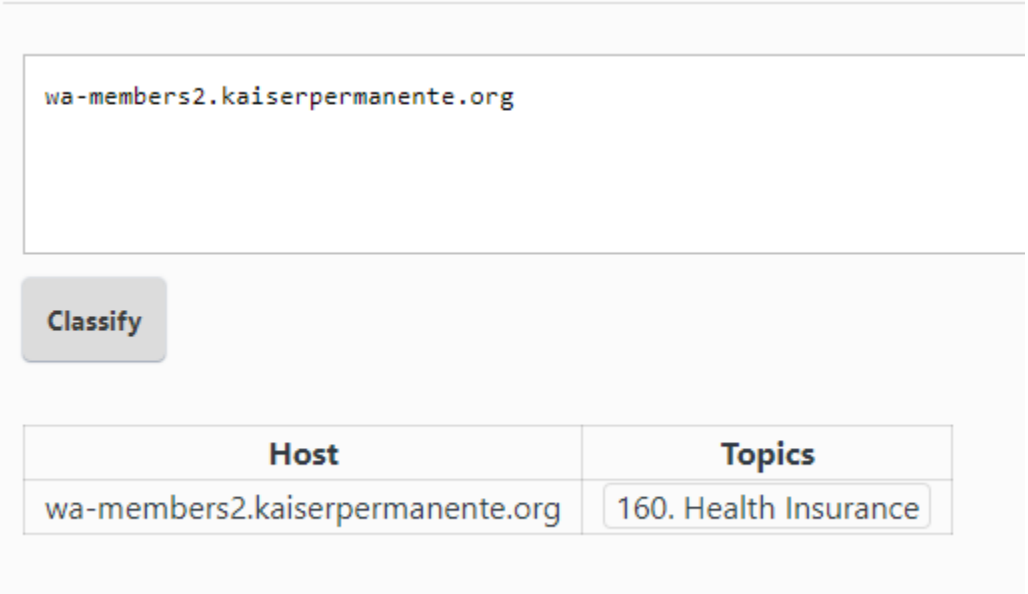
269. For example, when Plaintiffs navigated the Site, the Google code intercepted and redirected data to Google that Google then used to assign Topics to Plaintiffs and other Kaiser Plan Members, an example of which is below:

> if ('browsingTopics' in document && document.featurePolicy.allowsFeature('browsing-topics')) {\n fetch(\"https://pagead2.googlesyndication.com/pagead/buyside_topics/set/\", {**browsingTopics:true, keepalive:true}**)

As reflected above, the code string includes the following code: browsingTopics:true, Upon information and belief, this a default setting that is activated across Kaiser's Site. As Google explains to developers, this code "causes the browser to record the current page visit as observed by the caller,

so it can later be used in topics calculation."[72] As further reflected below, Google uses the page visit information to assign Plaintiffs and other Kaiser Plan Members with "Topic 160. Health Insurance" so that it can be determined if this is one of their top topics for the week and they can be targeted with ads by third party advertisers who pay Google for its targeted marketing capabilities.

Topics API Internals



270. Google also intercepts and receives other personally identifying information and personal and sensitive health information, including PHI, about Plaintiffs and other Kaiser Plan Members through GET requests sent to DoubleClick and POST transmissions to Google Analytics.

271. By way of example, when Plaintiff Jane Doe logged into the Portal on May 31, 2023, Google sent multiple GET requests to both googleads.g.doubleclick.net and google.com. These requests are essentially similar in nature. For example, the data sent via GET to Google servers at googleads.g.doubleclick.net is below:

> https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1685576958827&cv=11&fst=1685576958827&bg=ffffff&guid=ON&async=1&gtm=45be35v0&u_w=1366&u_h=768&url=https%3A%2F%2Fwa-member.kaiserpermanente.org%2Fhome%2F&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2F&label=Ump9CM7hr3IQosSlpAM&hn=www.googleadservices.com&frm=0&tiba=Secure%20Member%20Site%20%7C%20Kaiser%20Permanente%20Washington&auid=2067634156.1685575801&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B113.0.5

[72] *Topics API Developer's Guide*, Google https://developers.google.com/privacy-sandbox/relevance/topics/developer-guide (last visited Dec. 5, 2024).

672.127%7CChromium%3B113.0.5672.127%7CNot-A.Brand%3B24.0.0.0&uamb=0&uap=Windows&uapv=10.0.0&uaw=0&data=event%3Dconversion&rfmt=3&fmt=4

272. Similarly, on June 6, when Plaintiff John Doe logged into the Portal, Google also sent multiple GET requests to both googleads.g.doubleclick.net and google.com. These requests are also essentially similar in nature. For example, the data sent via GET to Google servers at googleads.g.doubleclick.net is below:

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1686076950094&cv=11&fst=1686076950094&bg=ffffff&guid=ON&async=1&gtm=45be35v0&u_w=1512&u_h=982&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fmedical-record&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&label=Ump9CM7hr3IQosSlpAM&hn=www.googleadservices.com&frm=0&tiba=Medical%20Record%20%7C%20Kaiser%20Permanente&auid=1088085833.1686076832&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event%3Dconversion&rfmt=3&fmt=4

273. The above GET requests includes the URL of the current site (blue highlight), the event type (highlighted in green)—in this case a conversion, as well as data about the browser and device that allows Google to produce a device fingerprint (highlighted in grey). The data sent to Google indicates the user successfully logged into the Portal.

274. When Plaintiff Jane Doe logged into the Portal, Google also used the POST method to transmit the following Google Analytics data to Google servers at www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70&gtm=45je35v0&_p=1252165919&cid=657412457.1685575799&ul=en-us&sr=1366x768&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.127%7CChromium%3B113.0.5672.127%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=Windows&uapv=10.0.0&uaw=0&ngs=1&_s=1&sid=1685575799&sct=1&seg=1&dl=https%3A%2F%2Fwa-member.kaiserpermanente.org%2Fhome%2F&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2F&dt=Secure%20Member%20Site%20%7C%20Kaiser%20Permanente%20Washington&en=page_view&_ee=1&_et=1

275. Similarly, when Plaintiff John Doe logged into the Portal, Google also used the POST method to transmit the following Google Analytics data to Google servers at www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70&gtm=45je35v0&_p=78753540&cid=1504176517.1686076832&ul=en-us&sr=1512x982&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.5672.126%7CNot-

A.Brand%3B24.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&ngs=1&_s=1&sid=1686076832&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fconsumer-interrupt.html&dt=My%20Health%20%7C%20Kaiser%20Permanente&en=page_view&_ee=1

276. The Google Analytics POST transmissions above include temporary and session IDs (cid, sid)—highlighted in yellow, an indication that the page loaded (green highlight), the URL of the current page (blue highlight), and information about the browser and device (grey highlight). As discussed above, device data allows Google to establish a device fingerprint to track devices across multiple websites. The data sent to Google indicates the user successfully logged into the Portal.

277. On June 6, 2023, when Plaintiff John Doe accessed his medical records from within the Portal, Google transmitted the fact that Plaintiff John Doe suffers from headaches and kidney stones through a GET requests back to Google's servers. Google also transmitted information about Plaintiff John Doe's physician back to its server.

278. For example, Doubleclick (and Google.com which was essentially similar) received the following information thorough GET requests from John Doe's medical records page:

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1686077690514&cv=11&fst=1686077690514&bg=ffffff&guid=ON&async=1&gtm=45be35v0&u_w=1512&u_h=982&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fmedical-record%2Fhealth-summary&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DICD%26queryICD10%3DR51.9%26label%3DHEADACHE%26groupName%3DHealth%2Bsummary&hn=www.googleadservices.com&frm=0&tiba=Health%20Summary%20%7C%20Medical%20Record%20%7C%20Kaiser%20Permanente&auid=1088085833.1686076832&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event%3Dgtag.config&rfmt=3&fmt=4

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1686079885283&cv=11&fst=1686079885283&bg=ffffff&guid=ON&async=1&gtm=45be35v0&u_w=1512&u_h=982&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fpages%2Fsearch%3Fquery%3Dkidney%2Bstones%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Ffront-door&hn=www.googleadservices.com&frm=0&tiba=Search%20%7C%20Kaiser%20Permanente&auid=875947082.1686079450&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.5672.126%7CNot-

A.Brand%3B24.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event%3Dgtag.config&rfmt=3&fmt=4

279. The above GET requests includes data about the browser and device (grey highlight) and URL data (blue highlight) reveals Plaintiff John Doe suffers from headaches (first GET data above) and kidney stones (second GET data above). This data can be used to better target ads.

280. While Plaintiff John Doe was accessing the medical records page, Google also used the POST method to transmit the following Google Analytics data to Google servers at www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70&gtm=45je35v0&_p=527624076&cid=1504176517.1686076832&ul=en-us&sr=1512x982&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&_eu=AEA&ngs=1&_s=2&sid=1686076832&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DICD%26queryICD10%3DR51.9%26label%3DHEADACHE%26groupName%3DHealth%2Bsummary&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fhconline%2Fie%2Finside.asp%3Flang%3Denglish%26mode%3Dsnapshot&dt=Search%20medical%20records&en=scroll&epn.percent_scrolled=90

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70&gtm=45je3650&_p=200520362&cid=1743351272.1686079450&ul=en-us&sr=1512x982&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&ngs=1&sid=1686079449&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fpages%2Fsearch%3Fquery%3Dkidney%2Bstones%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Ffront-door&dt=Search%20%7C%20Kaiser%20Permanente&_s=1

281. The POSTs above include a temporary session ID (cid)—highlighted in yellow, and information about the browser and device (grey highlight). The URLs of the current page (blue highlight) reveals Plaintiff John Doe suffers from headaches (first POST above) and kidney stones (second POST above). The data sent to Google can be used to better target ads.

282. On June 7, 2023 when Plaintiff John Doe requested an electronic copy of his medical records Google also used the POST method to transmit data to sb-ssl.google.com, including the following which specifically disclosed Plaintiff John Doe's name and other personally identifying information:

https://healthy.kaiserpermanente.org/ie/Documents/Released/Download?releaseId=WP-24F8cOV-2F43chhwz40hINz9AQ-3D-3D-24MVZtUU8nDZTmc44v1yuQuiofNjaDbbZ495l9c4zOCgI-3D&docId=WP-24wUdukuLzxp-2FfzWRYqPN1og-3D-3D-24gBNgJlReE8-2BNQgnAhLwt-2BrLft-2Bk2Dbuv2Y72rrLmVfs-3D&downloadedFileName=HealthSummary_Jun_07_2023.zip&idx=0"

ºhttps://healthy.kaiserpermanente.org/ie/Documents/Released/Download?releaseId=WP-24F8cOV-2F43chhwz40hINz9AQ-3D-3D-24MVZtUU8nDZTmc44v1yuQuiofNjaDbbZ495l9c4zOCgI-3D&docId=WP-24wUdukuLzxp-2FfzWRYqPN1og-3D-3D-24gBNgJlReE8-2BNQgnAhLwt-2BrLft-2Bk2Dbuv2Y72rrLmVfs-3D&downloadedFileName=HealthSummary_Jun_07_2023.zip&idx=0
127.0.0.1"Phttps://healthy.kaiserpermanente.org/ie/Documents/Released?from=DownloadMyRecord"R

Nhttps://healthy.kaiserpermanente.org/southern-california/secure/medical-record————"U

Qhttps://healthy.kaiserpermanente.org/southern-california/secure/my-medical-record————"†

• https://healthy.kaiserpermanente.org/southern-california/support/medical-requests.html?kp_shortcut_referrer=kp.org/requestrecords————————————"q

mhttps://healthy.kaiserpermanente.org/support/medical-requests.html?kp_shortcut_referrer=kp.org/requestrecords————————————"3

/https://www.kaiserpermanente.org/requestrecords————————————"!

https://kp.org/requestrecords————————————"¹

ehttps://healthy.kaiserpermanente.org/southern-california/secure/medical-record/download-health-record"Nhttps://healthy.kaiserpermanente.org/southern-california/secure/medical-record* 0JHealthSummary_Jun_07_2023.zipP————————————Zen-IHE_XDM/[redacted]/STYLE.XSL

IHE_XDM/[redacted]/DOC0038.XML

O-1 of 1 - My Health Summary.PDF

INDEX.HTM "

IHE_XDM/[redacted]/DOC0024.XML

IHE_XDM[redacted]/DOC0001.XML

IHE_XDM/[redacted]/DOC0005.XML

IHE_XDM/[redacted]/DOC0006.XML

IHE_XDM/[redacted]/DOC0007.XML

IHE_XDM[redacted]/DOC0008.XML

,F2pt¢• MGðàõ†ÆÌéÙ+□Æ“CLµ}S„Å ‰´8 @Â5(0 8 @ J-Chrome/113.0.5672.126/Mac OS XPX`• Ðà ø ¢”————————————

ºhttps://healthy.kaiserpermanente.org/ie/Documents/Released/Download?releaseId=WP-24F8cOV-2F43chhwz40hINz9AQ-3D-3D-24MVZtUU8nDZTmc44v1yuQuiofNjaDbbZ495l9c4zOCgI-3D&docId=WP-24wUdukuLzxp-2FfzWRYqPN1og-3D-3D-24gBNgJlReE8-2BNQgnAhLwt-2BrLft-2Bk2Dbuv2Y72rrLmVfs-3D&downloadedFileName=HealthSummary_Jun_07_2023.zip&idx=0
127.0.0.1"Phttps://healthy.kaiserpermanente.org/ie/Documents/Released?from=Dow

nloadMyRecord*ehttps://healthy.kaiserpermanente.org/southern-california/secure/medical-record/download-health-record0 9 ã•‰xBP————————————X p ¢————————

Phttps://healthy.kaiserpermanente.org/ie/Documents/Released?from=DownloadMyRecord 127.0.0.1"Ohttps://healthy.kaiserpermanente.org/ie/Documents/DownloadMyRecord?lang=english*ehttps://healthy.kaiserpermanente.org/southern-california/secure/medical-record/download-health-record0 9 ì•‰xBJehttps://healthy.kaiserpermanente.org/southern-california/secure/medical-record/download-health-recordP————————————X p ¢Š————————————

Ohttps://healthy.kaiserpermanente.org/ie/Documents/DownloadMyRecord?lang=english—— 127.0.0.10 9 °•‰xBB_

]https://healthy.kaiserpermanente.org/hconline/ie/inside.asp?lang=english&mode=downloadsummaryBQ

Ohttps://healthy.kaiserpermanente.org/ie/Documents/DownloadMyRecord?lang=englishJehttps://healthy.kaiserpermanente.org/southern-california/secure/medical-record/download-health-recordP

283. The above POST data includes the fact that Plaintiff John Doe requested an electronic copy of his medical records on June 7, 2023 (highlighted in green) and Plaintiff John Doe's ***first name*** (redacted above).

284. On June 6, 2023, when Plaintiff John Doe accessed the prescriptions page from within the Portal, Doubleclick and Google received the following information (which are essentially the same) through a GET request:

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1686077807673&cv=11&fst=1686077807673&bg=ffffff&guid=ON&async=1&gtm=45be35v0&u_w=1512&u_h=982&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-wellness%2Fdrug-encyclopedia%2Fdrug.259872&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fhconline%2Fie%2Finside.asp%3Flang%3Denglish%26mode%3Dsnapshot&hn=www.googleadservices.com&frm=0&tiba=omeprazole%2020%20mg%20capsule%2Cdelayed%20release%20%7C%20Kaiser%20Permanente&auid=1088085833.1686076832&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event%3Dgtag.config&rfmt=3&fmt=4

285. The above GET requests includes data about the browser and device (grey highlight), the current URL (blue), and data (pink) that reveals Plaintiff John Doe was prescribed Omeprazole 20mg delayed release. This data can be used to better target ads.

286. While Plaintiff John Doe was accessing the medications page, Google also used the POST method to transmit the following Google Analytics data to Google servers at www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70&gtm=45je35v0&_p=2017317913&cid=1504176517.1686076832&ul=en-us&sr=1512x982&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&ngs=1&_s=1&sid=1686076832&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-wellness%2Fdrug-encyclopedia%2Fdrug.259872&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fhconline%2Fie%2Finside.asp%3Flang%3Denglish%26mode%3Dsnapshot&dt=omeprazole%2020%20mg%20capsule%2Cdelayed%20release%20%7C%20Kaiser%20Permanente&en=page_view&_ee=1

287. The above POST includes data about the browser and device (grey highlight), the current URL (blue) and data (pink) that reveals Plaintiff John Doe was prescribed Omeprazole 20mg delayed release. This data can be used to better target ads.

288. When Plaintiff John Doe conducted a physician search from within the Portal the following GET request was sent to www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70&gtm=45je3650&_p=786057931&cid=1743351272.1686079450&ul=en-us&sr=1512x982&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&ngs=1&_s=2&sid=1686079449&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fphysicians%2Fevan-mosier-9630484&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fdoctors-locations&dt=Evan%20Alan%20Mosier%2C%20MD%20-%20Gastroenterology%20%7C%20Kaiser%20Permanente&en=user_engagement&_et=20792

289. GET request above includes temporary and session IDs (yellow highlight), information about the browser and device (grey highlight), the current URL (blue highlight), and addition data (pink highlight) which reveals Plaintiff John Doe searched for a gastroenterologist. This data can reveal Plaintiff John Doe's medical condition and can be used for better ad targeting. For example, the data can result in third parties serving ads for antacids or other digestive medications.

290. When Plaintiff Jane Doe conducted a search for "mental health" on the Site, Google used the POST method to transmit the following data to Google servers at www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70&gtm=45je35v0&_p=1051056236&cid=1313346476.1685578546&ul=en-us&sr=1366x768&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.127%7CChromium%3B113.0.5672.127%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=Windows&uapv=10.0.0&uaw=0&ngs=1&_s=1&sid=1685578545&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org

%2Fhealth-wellness%2Fmental-health%2Fhow-to-get-care&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&dt=How%20to%20get%20mental%20health%20care%20%7C%20Kaiser%20Permanente&en=page_view&_ee=1

291. The POST above includes temporary and session IDs (tid, cid, sid), highlighted in yellow, and information about the browser and device (grey highlight). The URL of the current page (blue highlight) reveals Plaintiff Jane Doe searched for the term "mental health." The data sent to Google can be similarly be used to better target ads.

292. Doubleclick's (and Google.com which was essentially similar) GET request from the search results page was:

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1685578748182&cv=11&fst=1685578748182&bg=ffffff&guid=ON&async=1&gtm=45be35v0&u_w=1366&u_h=768&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2F&hn=www.googleadservices.com&frm=0&tiba=Search%20%7C%20Kaiser%20Permanente&auid=1628977230.1685578549&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.127%7CChromium%3B113.0.5672.127%7CNot-A.Brand%3B24.0.0.0&uamb=0&uap=Windows&uapv=10.0.0&uaw=0&data=event%3Dgtag.config&rfmt=3&fmt=4

293. The above GET request includes data about the browser and device (grey highlight) and the URL of the page (blue highlight) reveals Plaintiff Jane Doe searched on the term "mental health." This data can similarly be used to better target ads.

294. When Plaintiffs John Doe II, John Doe III, Jane Doe II, Jane Doe III, Jane Doe IV, Jane Doe V, and Alexis Sutter accessed the Site and Apps, including the Patient Portal, their communications were similarly intercepted by Google.

295. On information and belief, the same type of information tracked, disclosed, and sent to Google for Plaintiffs has been tracked, disclosed, and sent to Google for other members of the Classes.

296. Whenever Kaiser Plan Members used the Site and Apps, Kaiser allowed Google to intercept the contents of their communications—including personal information, identifying information, and sensitive medical information—without their knowledge, consent, or authorization.

297. Kaiser knowingly redirected and disclosed Kaiser Plan Members' personally identifiable patient information, including their status as patients and the contents of their communications with Kaiser to Google.

298. Despite its legal obligations to keep this information and these communications private and confidential, Kaiser's use Google of code caused the redirection, interception, and transmission of the precise content of patients' communication with Kaiser to Google.

299. Kaiser's unauthorized redirection and disclosures to Google includes information that identifies Plaintiffs and Class Members as patients of Kaiser Permanente, and intercepts and/or aids in receiving and recording patient communications pertaining to or about specific medical conditions, health services, and specific doctors.

300. Kaiser's disclosures to Google occurred because Kaiser intentionally deployed Google code on its website, and that code "bugs" Kaiser Plan Members' web-browsers and causes personally identifiable patient information, as well as the contents of communications exchanged between Kaiser and its patients, to be redirected and sent to Google.

301. As deployed, Google code, as employed by Kaiser, functioned as a wiretap, Twitter as a third party wiretapper.

302. Kaiser purposefully collected Plaintiffs' and Class Members' personally identifiable information while also installing Google's code on its website and mobile applications and failing to prevent and/or aiding and abetting in that personally identifiable information being intercepted by Google thereby compromising Plaintiffs' and Class Members' privacy and the confidentiality of their personally identifiable information. Thus, by allowing Google to intercept Kaiser Plan Members' information and communications from the Site and Apps, Kaiser foreseeably harmed Plaintiffs and similarly situated Class Members.

303. Defendants knew or should have known that they were failing to comply with the applicable statutes and common law duties governing their conduct, and that Defendants' breach would cause Plaintiffs and Class Members to experience foreseeable harms associated with the unauthorized interception, disclosure, and use of their personal health information by Google.

c) Microsoft Bing Uses Kaiser Plan Members' Personally Identifying Information and PHI for its Own and Other Third Parties' Marketing

304. Microsoft Bing also collects a vast array of information about Users of the Site and Kaiser Permanente App so that it can use that data and better target specific individuals with ads.

305. For example, Microsoft Bing sells ads based on a User's search. So, if a Kaiser Plan Member searches for a medical condition such as cancer, that Kaiser Plan Member can thereafter be targeted with ads for cancer treatment centers.

306. Microsoft Bing is also a widely used ad platform that provides ad remarketing. Remarketing shows ads based on sites a user has previously visited. For example, a user who visits a website with Microsoft Bing code, and searches on pregnancy related topics, might then see ads for a Microsoft Bing advertiser's pregnancy related services on other websites.

307. Kaiser was aware of this when it installed the code on its Site and Kaiser Permanente App; indeed, Kaiser installed the Microsoft Bing code on its Site and Kaiser Permanente App to access this functionality.

308. Although Kaiser now admits it provided Microsoft Bing with Kaiser Plan Members' HIPAA-protected PHI through Microsoft code installed on the Site, Kaiser never entered into any contracts with Microsoft covering the offensive Microsoft Bing code installed on the Site and Kaiser Permanente App to ensure that Microsoft would not use the information they collected from the Site for Microsoft Bing's own or other third parties' advertising purposes. Although Kaiser and Microsoft entered into Business Associate Agreements covering other Microsoft products and services used by Kaiser, those Business Associate Agreements did not cover the relevant Microsoft Bing code on the Site and Kaiser Permanente App.

309. By way of example, on May 31, 2023, when Plaintiff Jane Doe logged into the Portal, Microsoft Bing received the following information through a GET request to bat.bing.com (color coded here and described in more detail below):

> https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=0449eabe-5045-4f9c-8768-afbe69c3f01a&sid=147515f0000b11ee937705de2bc479d9&vid=147628d0000b11eeabace7b017e63252&vids=0&msclkid=N&uach=pv%3D10.0.0&pi=918639831&lg=en-US&sw=1366&sh=768&sc=24&tl=Sign%20in&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fconsumer-sign-

on%23%2Fsignon&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fwashington%2Ffront-door&lt=22894&mtp=10&evt=pageLoad&sv=1&rn=404848

310. Alongside each of the GET requests to Bing were specific identifiers from cookies on Jane Doe's device, as well upon information, each Kaiser Plan Member's device, that identified the information received as pertaining specifically to the individual so that it could be matched to an advertising profile maintained by Microsoft Bing. For example, with the above GET request the following identifier was sent: MUID=0078ACA7BF5D61F3138BBF85BE706056

311. Upon information and belief, the MUID (or Machine Unique Identifier) is used by Microsoft Bing to identify specific browsers for advertising, site analytics, and other operations. The MUID can sync across domains and allows tracking of users by Microsoft Bing from website to website. The MUID is not an aggregate identifier; it is an individual identifier.

312. As another example, on June 6, 2023, when Plaintiff John Doe logged into the Portal, Bing received the following information through a GET request to bat.bing.com:

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=a57ffab9-4695-4ca1-967a-8733b98911d6&sid=9e997de0049911ee92ef43fd7e01cd75&vid=9e99a6f0049911ee89feed6f1e2c50f5&vids=0&msclkid=N&pi=918639831&lg=en-US&sw=1512&sh=982&sc=30&tl=My%20Health%20%7C%20Kaiser%20Permanente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fconsumer-interrupt.html&lt=1125&evt=pageLoad&sv=1&rn=258023

With the above GET request the following identifier was also sent: MUID=[redacted]

313. The Microsoft Bing GET request includes temporary and session IDs (mid, sid, vid)—highlighted in yellow above, an indication that the page loaded (green highlight), the URL of the page (blue highlight), and information about the browser and device (grey highlight). The data sent to Microsoft Bing indicates the user successfully logged into the Portal.

314. According to Microsoft Bing documentation, "the cookie in the relevant domain and IP address are always passed with every http request and not just via UET."[73] UET is Universal Event

[73] *FAQ: Universal Event Tracking*, Microsoft, https://help.ads.microsoft.com/apex/index/3/en/53056/ (last visited Dec. 5, 2024).

Tagging and it's the method used by Microsoft Bing to report advertiser activity on a Website. UET was installed on all pages viewed on the Kaiser Website, including within the Portal.

315. On June 6, 2023, when Plaintiff John Doe accessed his medical records from within the Portal, Microsoft Bing received the following information revealing that Plaintiff John Doe suffers from headaches and kidney stones through a GET requests back to its respective servers.

> https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=98019729-0e18-4699-bd10-1af56bb6e602&sid=9e997de0049911ee92ef43fd7e01cd75&vid=9e99a6f0049911ee89feed6f1e2c50f5&vids=0&msclkid=N&pi=918639831&lg=en-US&sw=1512&sh=982&sc=30&tl=Search%20medical%20records&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DICD%26queryICD10%3DR51.9%26label%3DHEADACHE%26groupName%3DHealth%2Bsummary&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fhconline%2Fie%2Finside.asp%3Flang%3Denglish%26mode%3Dsnapshot&lt=1469&evt=pageLoad&sv=1&rn=848129
>
> https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=5e099d19-6039-4641-8440-aa961649664c&sid=9e997de0049911ee92ef43fd7e01cd75&vid=9e99a6f0049911ee89feed6f1e2c50f5&vids=0&msclkid=N&pi=918639831&lg=en-US&sw=1512&sh=982&sc=30&tl=Search%20%7C%20Kaiser%20Permanente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fpages%2Fsearch%3Fquery%3Dkidney%2Bstones%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Ffront-door&lt=1013&evt=pageLoad&sv=1&rn=975174

316. The Bing GET requests above includes the same temporary and session IDs (mid, sid, vid) as the Portal page (yellow highlight), an indication that the page loaded (green highlight), and information about the browser and device (grey highlight), which identifies the computing device and allows for long term tracking. The GET request also transmitted to Microsoft Bing, the URL of the page (blue highlight), which in this case also includes the fact that Plaintiff John Doe suffers from headaches (first GET request above) and kidney stones (second GET request above). This data can be used to better target ads.

317. On June 6, 2023 when Plaintiff John Doe accessed the prescriptions page from within the Portal, Microsoft Bing received the following information through a GET request:

> https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=b5c83174-b4ea-4868-b60f-99002dea9a80&sid=9e997de0049911ee92ef43fd7e01cd75&vid=9e99a6f0049911ee89feed6f1e2c50f5&vids=0&msclkid=N&pi=918639831&lg=en-US&sw=1512&sh=982&sc=30&tl=omeprazole%2020%20mg%20capsule,delayed%20release%20%7C%20Kaiser%20Permanente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-wellness%2Fdrug-

encyclopedia%2Fdrug.259872&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fhconline%2Fie%2Finside.asp%3Flang%3Denglish%26mode%3Dsnapshot&lt=670&evt=pageLoad&sv=1&rn=325466

318. The Microsoft Bing GET request above includes the same temporary and session IDs (mid, sid, vid) as the Portal page (yellow highlight), an indication that the page loaded (green highlight), and information about the browser and device (grey highlight), which identifies the computing device and allows for long term tracking. The GET request also transmitted to Microsoft Bing, the fact that John Doe has been prescribed Omerprazole 20mg delayed release (pink highlight). This data can be used to better target ads. Indeed, discussed above, this GET request was accompanied by John Doe's MUID: MUID=[redacted]

319. On May 31, 2023 after Plaintiff Jane Doe logged out of the Portal, Plaintiff Jane Doe conducted a search using the search feature found on the upper right of the main page (Washington) of the Site. On the search results page, Microsoft Bing received the following information through a GET request:

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=fc8ef6c7-b66b-406b-b1e5-506f755f7359&sid=147515f0000b11ee937705de2bc479d9&vid=147628d0000b11eeabace7b017e63252&vids=0&msclkid=N&uach=pv%3D10.0.0&pi=918639831&lg=en-US&sw=1366&sh=768&sc=24&tl=Search%20%7C%20Kaiser%20Permanente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2F&lt=8071&mtp=10&evt=pageLoad&sv=1&rn=424250

320. The Microsoft Bing GET request above includes temporary and session IDs (mid, sid, vid) (yellow highlight), an indication that the page loaded (green highlight), and information about the browser and device (grey highlight). The GET request also transmitted to Microsoft Bing the URL of the page (blue highlight), which reveals Plaintiff Jane Doe's search on the term "mental health." Notably, although Plaintiff Jane Doe was logged out of the Portal, Microsoft Bing was still able to connect the fact that Plaintiff Jane Doe had communicated with Kaiser Permanente about mental health because it had created a digital fingerprint. This data can be used to better target ads.

321. Similarly, when Plaintiff John Doe logged out of the Portal and conducted a search for a physician on the Site the following GET request was sent to Microsoft Bing:

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=9f6a61d7-6328-4bd6-b325-0e5914ecbd5d&sid=9e997de0049911ee92ef43fd7e01cd75&vid=9e99a6f0049911ee89feed6f1e2c50f5&vids=0&msclkid=N&pi=918639831&lg=en-

US&sw=1512&sh=982&sc=30&tl=Find%20Doctors%20and%20Locations%20in%20Southern%20California%20%7C%20Kaiser%20Permanente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fdoctors-locations%23%2Fproviders%3Fzipcode%3D92395%26medical_specialty_label%3DPsychiatry%2520%2526%2520Neurology%3A%2520Neurology%2CPsychiatry%2520%2526%2520Neurology%3A%2520Psychiatry&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fdoctors-locations&lt=712&evt=pageLoad&sv=1&rn=110568

322. The Microsoft Bing GET request above includes temporary and session IDs (mid, sid, vid) (yellow highlight), an indication that the page loaded (green highlight), and information about the browser and device (grey highlight). The GET request also transmitted to Microsoft Bing the URL of the page (blue highlight), which reveals Plaintiff John Doe's search for a neurologist or psychiatrist in the 92395 zip code.

323. When Plaintiffs John Doe II, John Doe III, Jane Doe II, Jane Doe III, Jane Doe IV, Jane Doe V, and Alexis Sutter accessed the Site and Kaiser Permanente App, including the Patient Portal, their personally identifying information, PHI and communications were similarly intercepted by Microsoft Bing.

324. On information and belief, the same type of information tracked, disclosed, and sent to Microsoft Bing for Plaintiffs has been tracked, disclosed, and sent to Microsoft Bing for other members of the Classes.

325. Whenever Kaiser Plan Members used the Site and Kaiser Permanente App, Kaiser allowed Microsoft Bing to intercept the contents of their communications—including personal information, identifying information, and sensitive medical information—without their knowledge, consent, or authorization.

326. Kaiser knowingly redirected and disclosed Kaiser Plan Members' personally identifiable patient information, including their status as patients and the contents of their communications with Kaiser to Microsoft Bing.

327. Despite its legal obligations to keep this information and these communications private and confidential, Kaiser's use of Microsoft Bing code causes the redirection, interception, and transmission of the precise content of patients' communication with Kaiser to Microsoft Bing.

328. Kaiser's unauthorized redirection and disclosures to Microsoft Bing includes information that identifies Plaintiffs and Class Members as patients of Kaiser Permanente, and

intercepts and/or aids in receiving and recording patient communications pertaining to or about specific medical conditions, health services, and specific doctors.

329. Kaiser's disclosures to Microsoft Bing occurred because Kaiser intentionally deployed Microsoft Bing code on its website, and that code "bugs" Kaiser Plan Members' web-browsers and causes personally identifiable patient information, as well as the contents of communications exchanged between Kaiser and its patients, to be redirected and sent to Microsoft Bing.

330. As deployed, Microsoft Bing code, as employed by Kaiser, functioned as a wiretap, and Microsoft Bing as a third party wiretapper.

331. Kaiser purposefully collected Plaintiff and Class Members' personally identifiable information while also installing Microsoft Bing's code on its website and mobile applications and failing to prevent and/or aiding and abetting in that personally identifiable information being intercepted by Microsoft Bing thereby compromising Plaintiffs' and Class Members privacy and the confidentiality of their personally identifiable information. Thus, by allowing Microsoft Bing to intercept Kaiser Plan Members' information and communications from the Site and Apps, Kaiser foreseeably harmed Plaintiffs and similarly situated class members.

332. Defendants knew or should have known that they were failing to comply with the applicable statutes and common law duties governing their conduct, and that Defendants' breach would cause Plaintiffs and Class Members to experience foreseeable harms associated with the unauthorized interception, disclosure, and use of their personal health information by Microsoft Bing.

4. Kaiser Allows Its Members' Information and Communications to Be Intercepted While Using the Apps

333. Unbeknownst to Kaiser Plan Members and against their reasonable expectations, Kaiser also allows Quantum Metric, Adobe, Microsoft Bing, Google, Twitter, and Dynatrace to intercept Kaiser Plan Members' information and communications on the Kaiser Permanente App and/or the Kaiser Permanente Washington App.

a) The Kaiser Permanente App Caused Kaiser Plan Members' Individually Identifiable Personal Information, PHI and Confidential Communications to Be Transmitted to Adobe, Google, Microsoft Bing, Quantum Metric and Twitter

334. As reflected in the chart in Paragraph 103 above, which Kaiser produced in discovery (and is still subject to ongoing discovery and confirmation), Kaiser embedded code in the Kaiser Permanente App that causes Kaiser Plan Members' individually identifiable personal information, PHI and confidential communications to be transmitted to Adobe, Google, Microsoft Bing, and Twitter.

335. For example, on July 5, 2023, after Plaintiff John Doe was logged into the Kaiser Permanente App, Adobe, Microsoft Bing, Google, and Twitter all transmitted the fact that Plaintiff John Doe had a shoulder X-Ray in their GET and POST requests back to their respective servers.

336. For example, Adobe's POST request was:

{"requestId":"6472f0d6b00f42a08237efb30a436208","context":{"userAgent":"Mozilla/5.0 (iPhone; CPU iPhone OS 16_5_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148","clientHints":{},"timeOffsetInMinutes":-240,"channel":"web","screen":{"width":320,"height":693,"orientation":"portrait","colorDepth":32,"pixelRatio":3},"window":{"width":320,"height":523},"browser":{"host":"healthy.kaiserpermanente.org","webGLRenderer":"Apple GPU"},"address":{"url":"https://healthy.kaiserpermanente.org/southern-california/secure/search-medical-record?uri=search%3ahealth-encyclopedia&type=CPT&query=73030&label=X%2DRAY+SHOULDER","referringUrl":"https://healthy.kaiserpermanente.org/ie/inside.asp?mode=labdetail&eorderid=WP-24JO3eR3UxDisHiv7Y0JwpouLMwYNTlfWVwRYdzHiISmc-3D-240Wm-2BEg0CTZw6JiwFiZUTx5YqL6-2Bpia0C87YcG8EHhV4-3D"}},"id":{"marketingCloudVisitorId":"22568469190539506242433917920530928434"},"experienceCloud":{"audienceManager":{"locationHint":7,"blob":"6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"376DCC2C0069726A-059CD1F32377CB5D"}},"execute":{"pageLoad":{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:secure:search-medical-record","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":7692006,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg101v":27,"Seg516e":false,"Seg126v":false,"modval":6,"Seg21":100453,"Seg22":"","Seg24":"urn:kp:prodiem","Seg25":false,"Seg26":true,"entitlement-446":true,"pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"25","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":7692006,"Seg12":"ACTIVE","Seg101v":27,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","Seg103v":false}}},"prefetch":{"views":[{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:secure:search-medical-record","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":fals

e,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":7692006,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg101v":27,"Seg516e":false,"Seg126v":false,"modval":6,"Seg21":100453,"Seg22":"","Seg24":"urn:kp:prodiem","Seg25":false,"Seg26":true,"entitlement-446":true,"pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"25","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":7692006,"Seg12":"ACTIVE","Seg101v":27,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","Seg103v":false}}]}}

337. Microsoft Bing's GET request transmitted this same information to Microsoft, where it was stored on the company's bat.bing.com server:

GET /action/0?ti=5715144&Ver=2&mid=0fa19f20-cc67-481d-b44f-56a0eeb90d86&sid=eced51101b5111eebd4de38c20a30e4e&vid=eced67701b5111eea6131b899915cb55&vids=1&msclkid=N&pi=918639831&lg=en-US&sw=320&sh=693&sc=32&tl=Search%20medical%20records&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DCPT%26query%3D73030%26label%3DX%252DRAY%2BSHOULDER&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fie%2Finside.asp%3Fmode%3Dlabdetail%26eorderid%3DWP-24JO3eR3UxDisHiv7Y0JwpouLMwYNTlfWVwRYdzHiISmc-3D-240Wm-2BEg0CTZw6JiwFiZUTx5YqL6-2Bpia0C87YcG8EHhV4-3D&lt=2127&mtp=5&evt=pageLoad&sv=1&rn=699864 HTTP/1.1

338. Google's GET request transmitted this same information via googleads.g.doubleclick.net:

GET /pagead/viewthroughconversion/881418786/?random=1688574917452&cv=11&fst=1688574917452&bg=ffffff&guid=ON&async=1&gtm=45be36s0&u_w=320&u_h=693&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DCPT%26query%3D73030%26label%3DX%252DRAY%2BSHOULDER&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fie%2Finside.asp%3Fmode%3Dlabdetail%26eorderid%3DWP-24JO3eR3UxDisHiv7Y0JwpouLMwYNTlfWVwRYdzHiISmc-3D-240Wm-2BEg0CTZw6JiwFiZUTx5YqL6-2Bpia0C87YcG8EHhV4-3D&hn=www.googleadservices.com&frm=0&tiba=Search%20medical%20records&auid=1025871031.1688574917&data=event%3Dgtag.config&rfmt=3&fmt=4 HTTP/1.1

339. Twitter's GET request transmitted this same information via analytics.twitter.com and t.co:

GET /1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=d69ef292-e13b-41d1-86a7-7f70854dbd6a&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=14371743-a364-4c10-a8fc-c8cd0c09515b&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DCPT%26query%3D73030%26label%3DX%252DRAY%2BSHOULDER&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29 HTTP/1.1

340. Adobe, Microsoft Bing, Google, and Twitter all used GET and/or POST requests to transmit additional information about Plaintiff John Doe from within the Kaiser Permanente App, including the fact that Plaintiff John Doe is allergic to non-steroidal anti-inflammatory agents, that he suffers from headaches, and that he requires a vision prescription.

341. While Plaintiff John Doe was logged into the Kaiser Permanente App, Quantum Metric also intercepted and received information. Data was transmitted to Quantum Metric, including the fact that Plaintiff John Doe requires a vision prescription. Quantum Metric's POST request also contained an Adobe Marketing ID, allowing Plaintiff John Doe to be tracked across multiple platforms:

> POST /?T=B&u=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fmedical-record%2Fvision-prescriptions.mobile.html%3Flang%3Denglish%26stop_mobi%3Dyes%26adobe_mc%3DTS%253D1688575756%257CMCMID%253D32798239231981822676248079225746164835%257CMCORGID%253D9644AD4E5628B1ED7F000101%2540AdobeOrg&t=1688575779959&v=1688575780612&z=1&S=0&N=0&P=0 HTTP/1.1

342. As with the Third Party Wiretappers' code installed on the Site, Kaiser knowingly allowed these Third Party Wiretappers to intercept Plaintiffs' and other Kaiser Plan Members' personally identifying information and PHI from the time Kaiser installed their code on the Kaiser Permanente App until approximately November 2023 when Kaiser represented to this Court that it had disabled, deleted, or modified the Google code on the Site and Apps.

343. In fact, as Kaiser acknowledged in its recent disclosures to state and federal regulators, these online technologies provided by Google, Microsoft Bing, and Twitter installed on its mobile application collected HIPAA-protected PHI from Kaiser Health Plan Members, which until November 2023 included, inter alia, Kaiser Health Plan Members' IP addresses, names, information that could indicate a member was signed into a Kaiser account or service, information showing how the member interacted with and navigated through the website or mobile applications, and search terms used in the health encyclopedia.

344. Based on information and belief, when Plaintiffs John Doe II, John Doe III, Jane Doe II, Jane Doe III, Jane Doe IV, Jane Doe V, and Alexis Sutter accessed the Kaiser Permanente App,

their communications were similarly intercepted by Adobe, Microsoft Bing, Google, Twitter, and Quantum Metric.

345. On information and belief, the same type of information tracked, disclosed, and sent to Adobe, Microsoft Bing, Google, Twitter, and Quantum Metric was tracked, disclosed, and sent to these companies when other members of the Classes use the Kaiser Permanente App.

346. Kaiser purposefully collected Plaintiffs; and Class Members' personally identifiable information while also installing Adobe, Google, Microsoft Bing, Quantum Metric, and Twitter's code on its website and mobile applications and failing to prevent and/or aiding and abetting in that personally identifiable information being intercepted by Adobe, Google, Microsoft Bing, Quantum Metric and Twitter thereby compromising Plaintiffs' and Class Members' privacy and the confidentiality of their personally identifiable information. Thus, by allowing Adobe, Google, Microsoft Bing, Quantum Metric and Twitter to intercept Kaiser Plan Members' information and communications from the Site and Apps, Kaiser foreseeably harmed Plaintiffs and similarly situated Class Members.

347. Defendants knew or should have known that they were failing to comply with the applicable statutes and common law duties governing their conduct, and that Defendants' breach would cause Plaintiffs and Class Members to experience foreseeable harms associated with the unauthorized interception, disclosure, and use of their personal health information by Adobe, Google, Microsoft Bing, Quantum Metric and Twitter.

b) The Kaiser Permanente Washington App and Washington Site Caused Kaiser Plan Members' Individually Identifiable Personal Information, PHI and Confidential Communications to Be Transmitted to Adobe, Dynatrace, and Google

348. As reflected in the chart in Paragraph 103 above, which Kaiser produced in discovery (and is still subject to ongoing discovery and confirmation), Kaiser embedded code in the Kaiser Permanente Washington App and Washington Site that causes Kaiser Plan Members' individually identifiable personal information, PHI and confidential communications to be transmitted to Adobe, Dynatrace, and Google.

349. In addition to the Adobe and Google code discussed above, beginning in or around December 2015, Kaiser placed Dynatrace's "Application performance monitoring and management software" onto the Kaiser Permanente Washington App and Washington Site. Application performance monitoring ("APM") "is the practice of tracking key software application performance metrics using monitoring software and telemetry data."[74]

350. Dynatrace's APM platform provides "[m]obile and desktop application monitoring on mobile and desktop browsers to track user experience across platforms."[75] Like Quantum Metric, Dynatrace's APM platform captures Kaiser member's interactions with the Apps using Session Replay,[76] which is a "powerful tool" which can be used "to capture and visually replay the complete digital experience of every user."[77] Indeed, as Dynatrace explains, Session Replay records users' "interactions with your application and replay each click or tap in a movie-like experience."[78]

351. According to Kaiser's representations, which are subject to ongoing discovery, the purpose of the Dynatrace code was to perform "Platform Support – Performance and Support."

352. Similar to other Third Party Wiretappers, Dynatrace was permitted to use the information received from Kaiser for its own purposes. As Dynatrace's publicly available subscription agreement provides: "Dynatrace may monitor and collect Usage Data to improve Dynatrace's current and future offerings, and if aggregated and not identifying Customer or any individual, for industry analysis, benchmarking, and analytics."[79]

353. Kaiser Plan Members' data was being sent offsite to Dynatrace's servers until September 14, 2023, when Kaiser migrated the Dynatrace technology "to the on-premise deployment model offered by Dynatrace" after Plaintiffs initialed this action and moved for a preliminary injunction.[80] However, despite receiving PHI, which Kaiser tacitly acknowledged by moving the

[74] Dave Anderson, *What is APM? Application Performance Monitoring in a Cloud-native World*, Dynatrace (Mar. 26, 2024), https://www.dynatrace.com/news/blog/what-is-apm-2/.
[75] *Id.*
[76] *Id.*
[77] *Session Replay*, Dynatrace, https://docs.dynatrace.com/docs/platform-modules/digital-experience/session-replay (last visited Dec. 5, 2024).
[78] *Id.*
[79] *Subscription Agreement*, Dynatrace (Apr. 2023), https://assets.dynatrace.com/global/legal/Online-SA-April-2023-English.pdf.
[80] *See* Declaration of Bill Vourthis at 2-4, ECF No. 96.

Kaiser data to the on-premises deployment model, Kaiser did not have a Business Associate Agreement in place with Dynatrace.

354. For example, on July 5, 2023, when Plaintiff Jane Doe was logged into the Kaiser Permanente Washington App, Dynatrace intercepted and received information disclosing the fact that Plaintiff Jane Doe had a shoulder X-Ray. This information was intercepted by Dynatrace through a POST transmission and sent to bf12660qqg.bf.dynatrace.com:

> vv=3&va=8.241.1.1013&ap=591e7dfd-540c-4414-9bc0-8274741cd848&an=GroupHealth&ai=org.ghc.MyGroupHealth.Mobile&vn=5.2.1&vb=50201002&tv=1688580245590&tx=1688581822941&vi=93584938323505&sn=1&rm=3660&cp=ARM_64E&os=iOS%2016.5.1&mf=Apple&md=iPhone14%2C4&rj=g&ul=en_US&sw=960&sh=2079&sd=3&so=p&bl=77&fm=1&cr=T-Mobile&ct=m&np=5G&pt=0&tt=maios&dl=2&cl=2&mp=1&vs=1&fv=pl&et=30&na=https%3A%2F%2Fsmetrics.kaiserpermanente.org%2Fb%2Fss%2Fkfhkfhkpwamobileprod%2F0%2FIOSN020504020907%2Fs60219791&it=6&pa=0&s0=1088&t0=1481366&s1=0&t1=181&rc=200&bs=979&br=555&et=30&na=https%3A%2F%2Fwa-member2.kaiserpermanente.org%2FInterconnect-MyChartMobile-PRD%2FWCF%2FEpic.MyChartMobile%2FMyChartMobile.svc%2Frest_2017%2F0%2FTestResults%2FList&it=1&pa=0&s0=1091&t0=1481395&s1=0&t1=875&rc=200&bs=5796&br=22139&et=30&na=https%3A%2F%2Fwa-member2.kaiserpermanente.org%2FInterconnect-MyChartMobile-PRD%2FWCF%2FEpic.MyChartMobile%2FMyChartMobile.svc%2Frest_2018%2FGetMyChartUrl&it=1&pa=179&s0=1110&t0=1518572&s1=0&t1=1139&rc=200&bs=5948&br=1472&et=6&na=Touch%20on%20Ask%20a%20question&it=1&mo=0&ca=179&pa=0&s0=1106&t0=1518531&s1=1111&t1=1180&et=6&na=Touch%20on%20TableViewCell%20X-RAY%20shoulder%203V%20%400%3A3&it=1&mo=0&ca=178&pa=0&s0=1103&t0=1514139&s1=1105&t1=0&et=6&na=Touch%20on%20navigation%20back&it=1&mo=0&ca=177&pa=0&s0=1101&t0=1506019&s1=1102&t1=0&et=6&na=Touch%20on%20TableViewCell%20X-RAY%20shoulder%203V%20%400%3A3&it=1&mo=0&ca=176&pa=0&s0=1092&t0=1489670&s1=1094&t1=0&et=6&na=Loading%20GroupHealth.GroupHealthUITabBarController&it=1&mo=0&ca=173&pa=0&s0=1082&t0=1467076&s1=1085&t1=0&et=22&na=GroupHealth.HomeViewController&it=1&ca=175&pa=173&s0=1083&t0=1341984&s2=1084&t2=125100&s3=1087&t3=125711&et=22&na=GroupHealth.GroupHealthUITabBarController&it=1&ca=174&pa=173&s0=1080&t0=1341984&s2=1081&t2=125091&s3=1086&t3=125700

355. Dynatrace also intercepted and received information disclosing the fact Plaintiff Jane Doe had a mammogram, which was transmitted to Dynatrace through a POST transmission to bf12660qqg.bf.dynatrace.com:

> vv=3&va=8.241.1.1013&ap=591e7dfd-540c-4414-9bc0-8274741cd848&an=GroupHealth&ai=org.ghc.MyGroupHealth.Mobile&vn=5.2.1&vb=50201002&tv=1688580245590&tx=1688581943016&vi=93584938323505&sn=1&rm=3660&cp=ARM_64E&os=iOS%2016.5.1&mf=Apple&md=iPhone14%2C4&rj=g&ul=en_US&sw=960&sh=2079&sd=3&so=p&bl=77&fm=0&cr=T-Mobile&ct=m&np=5G&pt=0&tt=maios&dl=2&cl=2&mp=1&vs=1&fv=pl&et=30&na=https%3A%2F%2Fwa-member2.kaiserpermanente.org%2FInterconnect-MyChartMobile-PRD%2FWCF%2FEpic.MyChartMobile%2FMyChartMobile.svc%2Frest_2017%2F0%2F

TestResults%2FList&it=1&pa=0&s0=1133&t0=1683274&s1=0&t1=1002&rc=200&bs=6133&br=18544&et=6&na=Touch%20on%20TableViewCell%20EKG%20%400%3A21&it=1&mo=0&ca=185&pa=0&s0=1134&t0=1683806&s1=1136&t1=0&et=6&na=Touch%20on%20navigation%20back&it=1&mo=0&ca=184&pa=0&s0=1131&t0=1674266&s1=1132&t1=0&et=6&na=Touch%20on%20TableViewCell%20MAMMOGRAPHY%20SCREENING%203D%2C%20BILATERAL%20%400%3A17&it=1&mo=0&ca=183&pa=0&s0=1122&t0=1652016&s1=1124&t1=0&et=6&na=Touch%20on%20navigation%20back&it=1&mo=0&ca=182&pa=0&s0=1120&t0=1629868&s1=1121&t1=0&et=6&na=Loading%20GroupHealth.GroupHealthUITabBarController&it=1&mo=0&ca=180&pa=0&s0=1117&t0=1626769&s1=1119&t1=562&et=22&na=GroupHealth.GroupHealthUITabBarController&it=1&ca=181&pa=180&s0=1115&t0=1519083&s2=1116&t2=107685&s3=1118&t3=108248

356. The fact that Plaintiff Jane Doe suffers from restless leg syndrome was also intercepted and transmitted to Dynatrace at bf12660qqg.bf.dynatrace.com:

vv=3&va=8.241.1.1013&ap=591e7dfd-540c-4414-9bc0-8274741cd848&an=GroupHealth&ai=org.ghc.MyGroupHealth.Mobile&vn=5.2.1&vb=50201002&tv=1688580245590&tx=1688582667197&vi=93584938323505&sn=1&rm=3660&cp=ARM_64E&os=iOS%2016.5.1&mf=Apple&md=iPhone14%2C4&rj=g&ul=en_US&sw=960&sh=2079&sd=3&so=p&bl=75&fm=2&cr=T-Mobile&ct=m&np=5G&pt=0&tt=maios&dl=2&cl=2&mp=1&vs=1&fv=pl&et=30&na=https%3A%2F%2Fwa-member2.kaiserpermanente.org%2FInterconnect-MyChartMobile-PRD%2FWCF%2FEpic.MyChartMobile%2FMyChartMobile.svc%2Frest_2018%2FGetMyChartUrl&it=1&pa=0&s0=1543&t0=2318841&s1=0&t1=726&rc=200&bs=6005&br=1474&et=30&na=https%3A%2F%2Fsmetrics.kaiserpermanente.org%2Fb%2Fss%2Fkfhkfhkpwamobileprod%2F0%2FIOSN020504020907%2Fs76716014&it=6&pa=0&s0=1574&t0=2382147&s1=0&t1=188&rc=200&bs=1002&br=555&et=30&na=https%3A%2F%2Fwa-member2.kaiserpermanente.org%2FInterconnect-MyChartMobile-PRD%2FWCF%2FEpic.MyChartMobile%2FMyChartMobile.svc%2Frest_2018%2FGetMyChartUrl&it=1&pa=0&s0=1577&t0=2382191&s1=0&t1=617&rc=200&bs=5844&br=1374&et=30&na=https%3A%2F%2Fsmetrics.kaiserpermanente.org%2Fb%2Fss%2Fkfhkfhkpwamobileprod%2F0%2FIOSN020504020907%2Fs13525271&it=6&pa=0&s0=1593&t0=2410086&s1=0&t1=146&rc=200&bs=1005&br=555&et=30&na=https%3A%2F%2Fwa-member2.kaiserpermanente.org%2FInterconnect-MyChartMobile-PRD%2FWCF%2FEpic.MyChartMobile%2FMyChartMobile.svc%2Frest_2018%2FGetMyChartUrl&it=1&pa=0&s0=1594&t0=2410130&s1=0&t1=619&rc=200&bs=5839&br=1332&et=6&na=Loading%20GroupHealth.GroupHealthUITabBarController&it=1&mo=0&ca=279&pa=0&s0=1584&t0=2401338&s1=1589&t1=568&et=22&na=GroupHealth.MyHealthViewController&it=1&ca=281&pa=279&s0=1585&t0=2382710&s2=1586&t2=18635&s3=1588&t3=19196&et=22&na=GroupHealth.GroupHealthUITabBarController&it=1&ca=280&pa=279&s0=1582&t0=2382710&s2=1583&t2=18628&s3=1587&t3=19186&et=6&na=Touch%20on%20navigation%20back&it=1&mo=0&ca=277&pa=0&s0=1568&t0=2374384&s1=1571&t1=0&et=6&na=Touch%20on%20TableViewCell%20Essential%20hypertension%2C%20benign%20%400%3A1&it=1&mo=0&ca=276&pa=0&s0=1566&t0=2369408&s1=1567&t1=0&et=6&na=Touch%20on%20TableViewCell%20RLS%20%28restless%20legs%20syndrome%29%20%400%3A8&it=1&mo=0&ca=275&pa=0&s0=1558&t0=2359563&s1=1559&t1=0&et=6&na=Touch%20on%20TableViewCell%20RLS%20%28restless%20legs%20syndrome%29%20%400%3A8&it=1&mo=0&ca=274&pa=0&s0=1556&t0=2357113&s1=1557&t1=0&et=6&na=Touch%20on%20Health%20Issues&it=1&mo=0&ca=273&pa=0&s0=1554&t0=2344436&s1=1555&t1=0&et=6&na=Loading%20GroupHealth.GroupHealthUITabBarController&it=1&mo=0&ca=271&pa=0&s0=1551&t0=2334328&s1=1553&t1=0&et=22&na=GroupHealth.MyHealthViewController&it=1&ca=278&pa=277&s0=1569&t0=2319355&s2=1570&t2=55044&s3=1572&t3=55598&et=22&na=GroupHealth.GroupHealthUITabBarController&it=1&ca=272&pa=271&s0=1549&t0=2319355&s2=1550&t2=14972&s3=1552&t3=15557&et=6&na=Loading%20GroupHealth.GroupHealthUITabBa

rController&it=1&mo=0&ca=269&pa=0&s0=1537&t0=2310411&s1=1538&t1=0&et=22&na=GroupHealth.GroupHealthUITabBarController&it=1&ca=270&pa=269&s0=1535&t0=2284688&s2=1536&t2=25722&s3=1539&t3=26309

357. All of this information was sent with individually identifiable personal information, such as IP addresses sent along with POST transmissions and detailed recordings captured through Session Replay.

358. On information and belief, Dynatrace intercepted similar information when other members of the Classes use the Kaiser Permanente Washington App.

359. Kaiser purposefully collected Plaintiffs' and Class Members' personally identifiable information while also installing Adobe, Dynatrace, and Google's code on its website and mobile applications and failing to prevent and/or aiding and abetting in that personally identifiable information being intercepted by Adobe, Dynatrace, and Google thereby compromising Plaintiffs' and Class Members' privacy and the confidentiality of their personally identifiable information. Thus, by allowing Adobe, Dynatrace, and Google to intercept Kaiser Plan Members' information and communications from the Site and Apps, Kaiser foreseeably harmed Plaintiffs and similarly situated Class Members.

360. Defendants knew or should have known that they were failing to comply with the applicable statutes and common law duties governing their conduct, and that Defendants' breach would cause Plaintiffs and Class Members to experience foreseeable harms associated with the unauthorized interception, disclosure, and use of their personal health information by Adobe, Dynatrace, and Google.

C. Plaintiffs and Class Members Did Not Consent to Kaiser's Disclosure of Their Information and Communications to Third Parties

361. Kaiser does not ask Kaiser Plan Members who use its Site, Portal, and Apps, including Plaintiffs and members of the Classes, whether they consent to having the contents of their information and communications with Kaiser disclosed to the Third Party Wiretappers. Kaiser Plan Members are never actively told that their electronic communications are being wiretapped by Third Party Wiretappers.

362. Kaiser states in its Privacy Statement, under the heading "Internet Cookies," that:

> We and our service providers *may* place Internet "cookies" or similar technologies (JavaScript, HTML5, ETag) on the computer hard drives of visitors to the Site. Information we obtain helps us to tailor our Site to be more helpful and efficient for our visitors. For example, we are able to see the navigation path taken by users, and that information allows us to understand user success or challenges with the web experience. *The cookie consists of a unique identifier that does not contain information about your health history*. We use two types of cookies, "session" cookies and "persistent" cookies, along with other similar technologies.[81]

363. This does not disclose that Kaiser sends Plaintiffs and Class Members' information and communications to the Third Party Wiretappers.

364. First, these "third parties" are not defined in the Website Privacy Statement.

365. Second, disclosing that others *may* monitor certain information is not the same as disclosing that others *do in fact* collect user data in real time.

366. Third, Kaiser falsely claims that information about Kaiser Plan Members' health history is not being transmitted.

367. Fourth, alerting users to the possible use of "cookies . . . and other tracking technologies" does not put Kaiser Plan Members on notice of the use of technology like Session Replay, and other technology used by the Third Party Wiretappers, which, unlike first party cookies, (1) communicate information to an external server as a user navigates a website; (2) track users across devices; (3) are not easily disabled by users; and/or (4) essentially creates a recording of all the information that visitors provide or receive from Kaiser on the Site.

368. Fifth, disclosures to the Third Party Wiretappers are not made only for the purpose of tailoring the Kaiser website and mobile applications to be more helpful and efficient for Kaiser Plan Members who use the Site, Portal, and mobile applications, but are instead used for marketing purposes, including to produce targeted advertising for third parties.

369. Accordingly, Kaiser knowingly and willfully disclosed medical information without consent to the Third Party Wiretappers, for marketing purposes, including to produce targeted advertising for third parties.

[81] *Website and mobile application Privacy Statement*, Kaiser (last revised Oct. 2021), https://healthy.kaiserpermanente.org/privacy (emphasis added).

D. Plaintiffs' and Class Members' Health Information Has Actual, Measurable, Monetary Value

370. Kaiser Plan Members' confidential communications and information that Kaiser allows the Third Party Wiretappers to intercept has monetary value.

371. For example, one recent study asked over a thousand consumers from around the world what price they would demand of third parties for access to their data and found that passwords would fetch $75.80; health information and medical records themselves average $59.80; and in third, Social Security numbers were valued at $55.70.[82]

372. Some companies, such as Prognos Health, sell what they purport to be de-identified health information from millions of patients.[83]

373. Due to the difficulty in obtaining health information, illegal markets also exist for such data, with some reporting that health data can be "more expensive than stolen credit card numbers."[84]

E. Kaiser's Conduct Violates State and Federal Privacy Laws

374. Kaiser Plan Members have a reasonable expectation of privacy in their identifying information, personal and sensitive medical information and communications with Kaiser and its providers, rooted in state and federal privacy laws as well as Kaiser's express and implied contracts and disclosures. This includes a reasonable expectation that Kaiser Plan Members' identifying information, personal and sensitive medical information and communications with Kaiser and its providers will not be disclosed to or tracked by Third Party Wiretappers and will not be disclosed to third parties for marketing purposes.

375. Plaintiffs and Class Members reasonably believed their interactions with Kaiser on the Site, Portal, and mobile applications were private and would not be transmitted to third parties, recorded, or monitored for a later playback.

---

[82] Jonathan Weicher, *Healthcare hacks—how much is your personal information worth?*, Netlib Security, https://netlibsecurity.com/articles/healthcare-hacks-how-much-is-your-personal-information-worth/ (last visited Dec. 5, 2024).

[83] Press Release, *Prognos Health Announces Patent-Pending Technology* (Apr. 6, 2021), https://prognoshealth.com/about-us/news/press-release/prognos-health-announces-patent-pending-technology.

[84] Aarti Shahani, *The Black Market For Stolen Health Care Data*, NPR (Feb. 13, 2015, 4:55 am), https://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data.

376. The data collected by Kaiser identified specific web pages navigated and content viewed, and thus revealed personalized and sensitive information about Plaintiffs and Class Members, including sensitive personal and medical information.

377. Plaintiffs and Class Members did not have a reasonable opportunity to discover Defendants' unlawful and unauthorized connections and conduct because Kaiser did not disclose its actions nor seek consent from Plaintiffs or Class Members prior to making the transmissions to third parties.

378. 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.

379. For example, a study by Pew Research Center indicated that an overwhelming majority of Americans—approximately 79%—are concerned about how data is collected about them by companies.[85]

380. As Kaiser Plan Members, Plaintiffs and Class Members have a reasonable expectation of privacy that Kaiser, their health care provider, will not disclose the content of their personal and medical information and confidential communications with Kaiser and its providers to third parties without their express authorization.

381. Plaintiffs and Class Members' reasonable expectation of privacy in their personally identifiable data and communications exchanged with Kaiser and its providers is derived from several sources, including:

a. Kaiser's status as Kaiser Plan Members' health care provider;

b. Kaiser's common law obligation to maintain confidentiality of patient data and communications;

c. State and federal laws and regulations protecting the confidentiality of medical information;

d. State and federal laws protecting the confidentiality of communication and computer data;

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

e. Defendants' express promises of privacy and confidentiality; and

f. Defendants' implied promises of privacy and confidentiality.

382. Significantly, patient health care data in the United States is protected by federal law under HIPAA and its implementing regulations, which are promulgated by the HHS.

383. The HIPAA Privacy Rule, located at 45 CFR § 160 and Subparts A and E of § 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[86]

384. The Privacy Rule broadly defines "protected health information" ("PHI") as "individually identifiable health information" ("IIHI") that is "(i) [t]ransmitted by electronic media; (ii) [m]aintained in electronic media; or (iii) [t]ransmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

385. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

386. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

387. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health

[86] *The HIPAA Privacy Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited Dec. 5, 2024).

information relating to an individual." 42 U.S.C. § 1320d-6. The statute states that a "person . . . shall be considered to have obtained or disclosed individually identifiable health information . . . if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization." *Id.*

388. Guidance from HHS confirms that patient status is protected by HIPAA, which provides

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data. . . . ***If such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.***[87]

389. HHS has previously instructed that patient status is protected by the HIPAA Privacy Rule:

a. "[T]he sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

b. "[A] covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and

d. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

F. Kaiser Disregarded Plaintiffs' and Class Members' Privacy Rights With Other Web Technologies as well as with the Third Party Wiretappers

390. As Kaiser Plan Members, Plaintiffs and Class Members have a reasonable expectation of privacy that Kaiser will not disclose that they are Kaiser insured and patients receiving treatment from Kaiser Permanente to third parties without their express authorization.

[87] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* at 5, HHS (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf. (emphasis added).

391. As a healthcare provider and insurer, Kaiser has a duty to keep patients' medical information confidential, yet time and again breached this duty in order to enhance its marketing opportunities. As stated by Kaiser Permanente's Chief Marketing Officer in a September 2023 interview, "I really want myself and my team to be willing to innovate, to be bold, to take risks, to fail fast, to really lead with a growth mindset because that's how you get better."[88] Unfortunately for Kaiser Permanente members, one of the "risks" taken with this growth marketing mindset is the trampling of patient privacy rights and the duty to maintain confidentiality.

392. [redacted].

393. [redacted].

[88] *CMO Spotlight | Kristy LoRusso - Kaiser Permanente*, Setup, https://setup.us/blog/cmo-spotlight-kristy-lorusso-kaiser-permanente (last visited Dec. 5, 2024).

394. [redacted].

395. [redacted]

396. [redacted]

397. [redacted].

398. For example, through a process called "cookie syncing" or "cookie mapping," Kaiser identified Kaiser Permanente Members to advertisers through the usage of unified advertising profiles. As discussed above, many of the Third Party Wiretappers use pseudonymous identifiers, at times captured in cookies, to track users and their devices. Just as a user's name may not be part of a

social security number or phone number, those numbers are stored in directories that can identify the individual. A pseudonymous advertising identifier is no different.

399. Kaiser's integration of the Trade Desk Pixel into its Site provided such a service. According to TradeDesk, its "partners [*i.e.*, Kaiser] will leverage the adsrvr.org [the Trade Desk] endpoint as an ID issuing service. Adsrvr.org in turn will work towards propagating new users across participants so that we improve the coverage and match rate for all partners that are using TDID as their primary ID."[89]

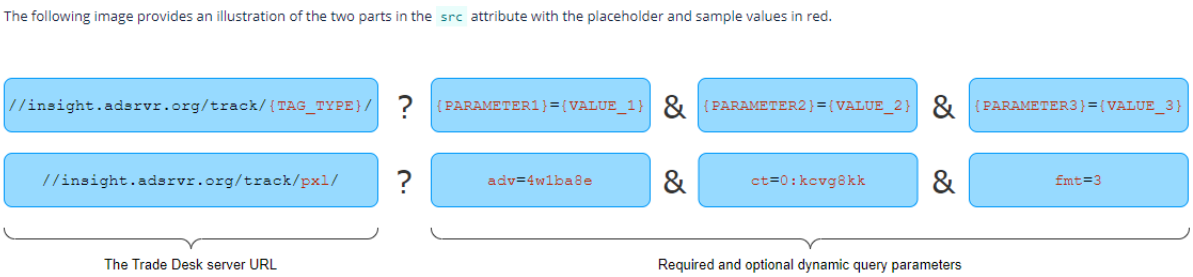
400. The specific mechanics of the Trade Desk Pixel are as follows.

401. Like the Third Party Wiretapper Pixels, the Trade Desk Pixel fired when a webpage was loaded, sending a GET request to the Trade Desk's servers.

402. For example, when John Doe was logged into the Kaiser Site, the Trade Desk Pixel sent the following GET request to Trade Desk's servers.

request":{"method":"**GET**","url":"**https://insight.adsrvr.org/track/pxl/?adv=5hlxcry&ct=0:g4bze3e&fmt=3**","httpVersion":"HTTP/1.1","cookies":[],"headers":[{"name":"host","value":"insight.adsrvr.org"},{"name":"connection","value":"keep-alive"}

403. Trade Desk parses the URL into its component parts:[90]



404. Following the Trade Desk server URL, "**https://insight.adsrvr.org/track/pxl/**" (pxl for pixel), there are four required parameters. First is the "adv" parameter, which is the "[t]he platform ID for the advertiser that owns the tracking tag".[91] In the above, the "adv" parameter is set to "5hlxcry", *i.e.*, "**adv=5hlxcry**." Second is the "ct" parameter, which is the "image pixel attribute"

---

[89] *Unified ID Adoption Guidelines for DMPs* at 2, The Trade Desk (Oct. 2019), https://www.thetradedesk.com/assets/global/Unified-ID-Adoption-Guidelines-for-DMPs-v1.3.pdf.
[90] *Tracking Tags*, The Trade Desk, https://partner.thetradedesk.com/v3/portal/data/doc/TrackingTagsOverview (last visited Dec. 5, 2024).
[91] *Static Tracking Tag*, The Trade Desk, https://partner.thetradedesk.com/v3/portal/data/doc/TrackingTagsStatic (last visited Dec. 5, 2024).

and is described as a "legacy parameter; the value doesn't change." In the above, the "ct" parameter is set to "0". Third is the "{TRACKING_TAG_ID}" parameter and is "[t]he platform ID for the tracking tag." Above the "{TRACKING_TAG_ID}" parameter is set to "**g4bze3e.**" Most importantly here, the fourth component is the "fmt" parameter. When the "fmt" parameter is set to "3", *i.e.*, "**fmt=3**", this directs the Trade Desk to "initiate cookie synching".[92] If the "fmt" parameter is instead set to "4", then it stops cookie syncing, though that would be contrary to the purpose of inserting such code on the Site.

405. The Trade Desk's server responds to this request by providing the individual user's pseudonymous Trade Desk ID, denoted in the code as "TDID", (presumably shorthand for "Trade Desk ID") and places this identifier on the user's browsing device.

"name":"cookie","value":"TDID=d7e65f1d-ab22-4a5a-bec9-dded2ec0b803;

406. Upon information and belief, the TDID was then sent by the Trade Desk to an advertiser for its own mapping. After different requests were sent to the Trade Desk by John Doe's browser different advertisers received John Doe's identifier.[93] For example:

The Rubicon Project:[94]

https://pixel.rubiconproject.com/tap.php?v=8981&nid=2307&put=**d7e65f1d-ab22-4a5a-bec9-dded2ec0b803**&gdpr=0&gdpr_consent=&expires=30&next=https%3A%2F%2Fmatch.adsrvr.org%2Ftrack%2Fcmf%2Frubicon

Yahoo:

https://ups.analytics.yahoo.com/ups/55953/sync?uid=**d7e65f1d-ab22-4a5a-bec9-dded2ec0b803**&_origin=1&redir=true&gdpr=0&gdpr_consent=

Google / Doubleclick:

https://cm.g.doubleclick.net/pixel?google_nid=TheTradeDesk&google_cm&google_sc&google_hm=ZDdlNjVmMWQtYWIyMi00YTVhLWJlYzktZGRlZDJlYzBiODAz&gdpr=0&gdpr_consent=&ttd_tdid=**d7e65f1d-ab22-4a5a-bec9-dded2ec0b803**

AppNexus:

https://ib.adnxs.com/getuid?https%3a%2f%2fmatch.adsrvr.org%2ftrack%2fcmf%2fappnexus%3fttd%3d1%26anid%3d%24UID&ttd_tdid=**d7e65f1d-ab22-4a5a-bec9-dded2ec0b803**

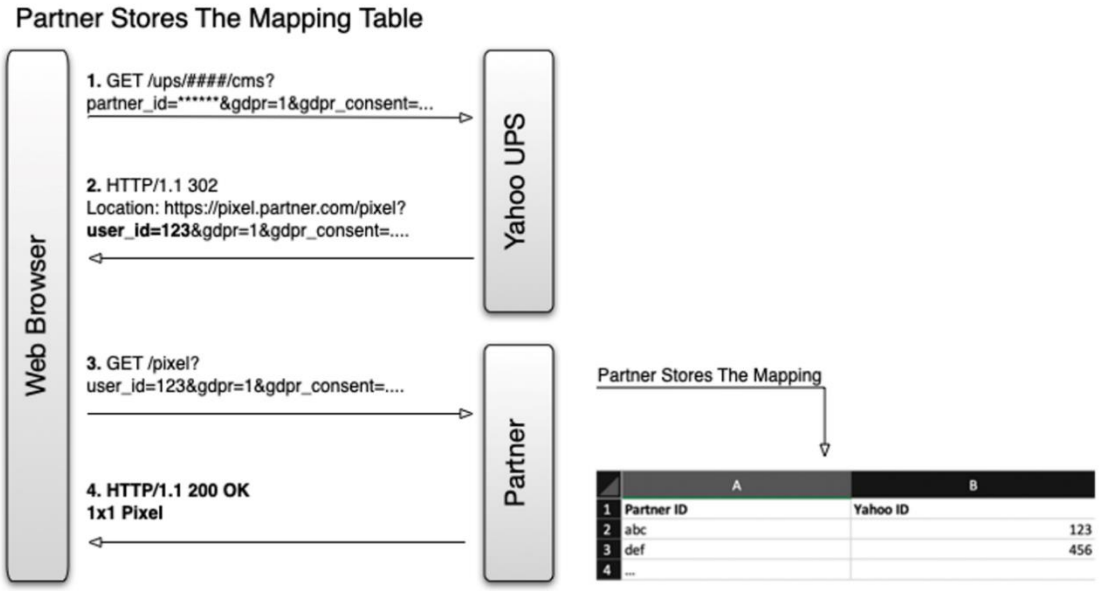
---

[92] *Id.*

[93] The Trade Desk also provide a "TDCPM" value which upon information and belief is an identifier for the browser device.

[94] The Rubicon Project is part of Magnite, Inc. which describes itself as "Magnite is the world's largest independent sell-side advertising company. Publishers use our technology to monetize their content across all screens and formats including CTV, online video, display, and audio." *Investor Home*, Magntie, https://investor.magnite.com/ (last visited Dec. 5, 2024).

407. Yahoo, one of the recipients, illustrates the cookie syncing / cookie mapping process as:



408. As illustrated by the above, and as described by the Trade Desk, Trade Desk is operating as "ID issuing service" by simply matching patients to their unique Trade Desk identifier.

409. The recipients—third parties—of the TDID from Kaiser's servers can and do use the TDID to target that patient. Not only do these vendors use this data for their own purposes, so does the Trade Desk.

410. In its Privacy Policy, the Trade Desk indicates that:

- "We disclose mappings of pseudonymous IDs with clients and partners that use our device graphs.
- We disclose cookie values to other advertising technology platforms so that they may match their value to our value."[95]

411. Further, as part of its "ID issuing service," the Trade Desk is collecting information at the same time it is providing the TDID. The Trade Desk states the following with regard to the TDID cookie:

> Cookies help us by enabling our ability to distinguish between, recognize, and store data about unique web browsers and devices, and to store data on our servers for

[95] *Privacy and The Trade Desk Platform*, The Trade Desk (Apr. 12, 2024), https://www.thetradedesk.com/us/privacy.

> the advertising purposes described here. Our cookie domain is adsrvr.org. The Trade Desk ID (TDID) is used to recognize web-browser profiles over time across sites. The TDID has a lifespan of 1 year from the time you last received an ad powered by Platform. This lifespan may be updated each time your browser encounters our Platform.
>
> In order to be able to transmit requests for ads and other data about users or devices between sellers and buyers, and to help show you ads that match your likely interests, we engage in cookie syncing, meaning that we match our TDID to clients' and partners' cookie IDs. We also use a cookie to store a related opt-out choice, when users opt out of cookie based targeted advertising.[96]

412. The Trade Desk's Privacy Policy continues to describe its usage of data it receives for TDIDs:

> Personalised profiles. As part of our Platform, we may create and use user profiles associated with pseudonymous identifiers. This means that we look at the information associated with the IDs and with the requests for ads, such as the content in which the ad is shown, the time, the geographic location, and the type of device. Sometimes we use information about whether or how users responded to ads to find other users who would respond to ads. We apply various computational methods on this information to find groupings of IDs that may have certain common interests or characteristics, such as "clothing," "sports," "travel," "male," "25-54," and so on. Our Platform also enables data suppliers to bring data to the Platform that our clients can use on the Platform to improve their ad campaigns.
>
> Clients can bring their own data to the Platform for their own personalisation. Their sources and methods for acquiring this data vary and are subject to our clients' own policies and legal obligations. We contractually prohibit certain types of data from being introduced onto the Platform, such as certain sensitive data. Our contracts prohibit clients and partners from using data on the Platform that is from or about users that they know are children.[97]

413. When Kaiser implemented the Trade Desk Pixel into its website, it allowed a third party to identify Kaiser's patients by their advertising ID (the TDID) and collect data about Kaiser patients. Not only was this advertising ID retrieved, but in the process, the third party was provided data which it could use for its own benefit in the course of its business as an identification broker and issuer. This advertising ID was then sent to other advertisers so that they could associate that ID with Kaiser Permanente for their own advertising purposes.

414. Moreover, due to the many overlapping technology services implemented on Kaiser's Site and Apps, the Trade Desk was not alone in this sort of conduct. For example, another integrated

[96] *Id.*
[97] *Id.*

technology Kaiser implemented was Adform. In Adform's Privacy Policy it states under the heading of "What Information Do We Collect and Use":[98]

> 1. Reporting, measurement, forecasting, attribution
>
> Brief explanation
>
> Specific processing activities may be, for example:
>
> We use combined data from cookies and the number of impressions to predict user/audience trends.
>
> We gather IDs when a user visits an advertiser's website through tracking the user's online activity.
>
> For more information, please read here. [no hyperlink provided]
>
> Data Categories
>
> 1st Party IDs, Cookie IDs, and technical data related to these IDs (e.g. impressions, clicks, conversions, approximate geolocation, timestamp, URL, device information, browser information), IP address.
>
> Related Adform Product and/or Service
>
> Buy Side, Sell Side, DMP.
>
> Legal bases
>
> We process this data by default on the basis of our legitimate interest. However, the **publisher on whose site we are integrated with our product or service can decide to obtain your consent**. In this case, we process the data based on your consent.
>
> * * *
>
> 4. Develop and Improve products (IAB Purpose 10)
>
> Brief explanation
>
> Personal data about how you use Adform clients' websites or apps, like how you engage with ads or content, can be really valuable for improving Adform products and services and creating new ones based on users' activity online.
>
> Data Categories
>
> 1st Party IDs, Cookies IDs and other identifiers as applicable, as well as real-time data (e. g. information about the page content, app type).
>
> Related Adform Product and/or Service
>
> Buy Side, Sell Side, Ad server, DMP.
>
> Legal bases
>
> We process this data by default on the basis of our legitimate interest. However, the **publisher on whose site we are integrated**

[98] *Adform Product and Services Privacy Policy*, Adform (May 1, 2024), https://site.adform.com/privacy-center/platform-privacy/product-and-services-privacy-policy/ (emphasis added).

> **with our product or service can decide to obtain your consent**. In this case, we process the data based on your consent.

5. Synchronize our Service with other online advertising services (Link different End User devices) (IAB Feature 2)

Brief explanation

> We might use Cookie IDs and other IDs to connect our Service with other online advertising services. **This is an essential part of the digital advertising world because it helps our clients combine data from different advertising service providers**. No other personal data is used for this purpose.

Data Categories

> 1st Party IDs, Cookies IDs and other identifiers as applicable.

Related Adform Product and/or Service

> Buy Side, Sell Side, Ad server, DMP.

Legal bases

> We process this data by default on the basis of our legitimate interest. However, the **publisher on whose site we are integrated with our product or service can decide to obtain your consent**. In this case, we process the data based on your consent.

415. Similar to the Trade Desk, Adform takes cookie information and syncs the identifier across databases in order to identify the specific patient. As noted by Adform, "this is an essential part of the digital advertising world."[99] Without this function, individuals would not be able to be targeted on their specific phone or device. Moreover, all of the above activities are taken by Adform ***by default*** for the data it receives. Adform notes that it also does these activities on the basis of consent provided to the publisher, *i.e.*, Kaiser.

416. Upon information and belief, due to Adform's integration into Kaiser's Sites and Apps, the Kaiser patient data received by Adform was used for its own purposes for such as reporting, measurement, forecasting, and attribution; developing and improving its own products; and synchronize Adform with other online advertising services (link different End User devices).

417. As described above, nowhere in Kaiser's Privacy Statement does it state that it allows advertisers to "sync" or "map" cookies with patient identities and / or their devices. Nor does it state

[99] *Id.*

that it allows third parties such as Adform to use patient information to improve their own services with the data received from Kaiser's Site and Apps.

418. The rampant dissemination of Kaiser patient information to entities that can use this information for their own purposes and the insertion of the Third Party Wiretapper code onto the Site and Apps all stems from Kaiser's goal of using its patient data for its own growth. Kaiser knowingly inserted this code and provided this data to third parties while failing to protect its patients' confidentiality.

V. TOLLING

419. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

420. The statutes of limitations applicable to Plaintiffs and the Classes' claims were tolled by Defendants' conduct and Plaintiffs and Class Members' delayed discovery of their claims.

421. As alleged above, Plaintiffs and members of the Classes did not know, and could not have known, when they used the Kaiser Site and/or Portal that Kaiser was disclosing their information and communications to third parties. Plaintiffs and members of the Classes could not have discovered Kaiser's unlawful conduct with reasonable diligence.

422. Kaiser secretly incorporated the Third Party Wiretappers' code into the Site, Portal, and Apps, providing no indication to Kaiser Plan Members and Site and App users that their communications would be disclosed to these third parties.

423. Kaiser had exclusive and superior knowledge that the Third Party Wiretappers' code incorporated on its Site, Portal, and Apps would disclose Kaiser Plan Members' protected and private information and confidential communications, yet failed to disclose to Kaiser Plan Members and Site and App users, including Plaintiffs and members of the Classes, that by interacting with the Kaiser Site, Portal, or Apps that Plaintiffs and Class Members' patient status, personal information, sensitive health information, and confidential communications would be disclosed to third parties.

424. [redacted].

425. Kaiser also affirmatively withheld and knowingly failed to disclose this conduct, despite being required to do so under the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, and comparable state laws, even after it publicly admits to knowing of these violations.

426. As Kaiser's notice to the Washington Attorney General makes clear, Kaiser understood its obligations to report when Kaiser Plan Members' PHI had been exposed, but nevertheless failed to notify regulators or the public until April 12, 2024. Despite an affirmative obligation to provide notification to Plaintiffs and Class Members, Kaiser knowingly withheld this information.

427. Plaintiffs and members of the Classes could not with due diligence, have discovered the full scope of Kaiser's conduct because the incorporation of the Third Party Wiretappers' code is highly technical and there were no disclosures or other indication that would inform a reasonable consumer or user that Kaiser was disclosing and allowing the interception of such information to these third parties in the manner and for the purposes alleged here.

428. The earliest Plaintiffs and Class Members could have known about Defendants' conduct was shortly before the filing of this Complaint.

VI. CLASS ACTION ALLEGATIONS

429. Plaintiffs bring this action pursuant to Federal Rules of Civil Procedure 23(a) and 23(b)(2) and/or (b)(3) on behalf of the following Class and Sub-Classes:

Kaiser Operating States Class: All Kaiser Plan Members in the Kaiser Operating States who used the Kaiser website or mobile applications.

California Sub-Class: All Kaiser Plan Members who are residents of the State of California and used the Kaiser website or mobile applications.

Colorado Sub-Class: All Kaiser Plan Members who are residents of the State of Colorado and used the Kaiser website or mobile applications.

District of Columbia Sub-Class: All Kaiser Plan Members who are residents of the District of Columbia and used the Kaiser website or mobile applications.

Georgia Sub-Class: All Kaiser Plan Members who are residents of the State of Georgia and used the Kaiser website or mobile applications.

Maryland Sub-Class: All Kaiser Plan Members who are residents of the State of Maryland and used the Kaiser website or mobile applications.

Oregon Sub-Class: All Kaiser Plan Members who are residents of the State of Oregon and used the Kaiser website or mobile applications.

Virginia Sub-Class: All Kaiser Plan Members who are residents of the Commonwealth of Virginia and used the Kaiser website or mobile applications.

Washington Sub-Class: All Kaiser Plan Members who are residents of the State of Washington and used the Kaiser website or mobile applications.

Kaiser Operating States Breach of Contract Sub-Class: All Kaiser Plan Members in the Kaiser Operating States who used the Portal on the Kaiser website or mobile applications.

California Breach of Contract Sub-Class: All Kaiser Plan Members who are residents of the State of California and used the Portal on the Kaiser website or mobile applications.

Colorado Breach of Contract Sub-Class: All Kaiser Plan Members who are residents of the State of Colorado and used the Portal on the Kaiser website or mobile applications.

District of Columbia Breach of Contract Sub-Class: All Kaiser Plan Members who are residents of the District of Columbia and used the Portal on the Kaiser website or mobile applications.

Georgia Breach of Contract Sub-Class: All Kaiser Plan Members who are residents of the State of Georgia and used the Portal on the Kaiser website or mobile applications.

Maryland Breach of Contract Sub-Class: All Kaiser Plan Members who are residents of the State of Maryland and used the Portal on the Kaiser website or mobile applications.

Oregon Breach of Contract Sub-Class: All Kaiser Plan Members who are residents of the State of Oregon and used the Portal on the Kaiser website or mobile applications.

Virginia Breach of Contract Sub-Class: All Kaiser Plan Members who are residents of the Commonwealth of Virginia and used the Portal on the Kaiser website or mobile applications.

Washington Breach of Contract Sub-Class: All Kaiser Plan Members who are residents of the State of Washington and used the Portal on the Kaiser website or mobile applications.

430. Excluded from the Class and Sub-Classes are Defendants and their parents, subsidiaries, and corporate affiliates. Plaintiffs reserve the right to revise the definition of the Class and Sub-Classes based upon subsequently discovered information and reserves the right to establish additional Sub-Class where appropriate. The Class and Sub-Classes are collectively referred to herein as the "Class" or "Classes."

431. The Classes are so numerous that joinder of all members is impracticable. Plaintiffs believe that there are millions of proposed members of the Classes throughout the United States.

432. Common questions of law and fact exist as to all members of the Classes and predominate over any issues solely affecting individual members of the Classes. The common and predominating questions of law and fact include, but are not limited to:

- Whether Defendants' acts and practices violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq*.;
- Whether Defendants' acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*.;
- Whether Defendants' acts and practices violated California's Constitution, Art. 1, § 1;

- Whether Defendants' acts and practices violated California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.10;
- Whether Defendants' acts and practices violated District of Columbia Consumer Protection Procedures Act, D.C. Code §§ 28-3901, *et seq.*;
- Whether Defendants' acts and practices violated the District of Columbia Consumer Security Breach Notification Act, D.C. Code §§ 28-3851, *et seq.*;
- Whether Defendants' acts and practices violated Georgia Computer Systems Protection Act, Ga. Code Ann. § 16-9-93;
- Whether Defendants' acts and practices violated Georgia Insurance and Information Privacy Protection Act, Ga. Code Ann. § 33-39-1, *et seq.*;
- Whether Defendants' acts and practices violated Maryland Wiretapping and Electronic Surveillance Act, Md. Code Ann., Cts. & Jud. Proc. §§ 10-401, *et seq.*;
- Whether Defendants' acts and practices violated the Oregon Unlawful Trade Practices Act, Or. Rev. Stat. §§ 646.605, *et seq.*;
- Whether Defendants' acts and practices violated the Oregon Consumer Information Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*;
- Whether Defendants' acts and practices violated Virginia Computer Crimes Act, Va. Code Ann. §§ 18.2-152.1, *et seq.*;
- Whether Defendants' acts and practices violated Virginia Insurance Information and Privacy Protection Act, Va. Code Ann. §§ 38.2-600, *et seq.*;
- Whether Defendants' acts and practices violated the Washington Privacy Act, Wash. Rev. Code §§ 9.73, *et seq.*;
- Whether Defendants' acts and practices violated the Washington Health Care Information Act, Wash. Rev. Code § 70.02.005, *et seq*;
- Whether Defendants' acts and practices violated the Washington Consumer Protection Act, §§ 19.86, *et seq.*;
- Whether Defendants' acts and practices violated the Washington Data Breach Act ("DBA"), Wash. Rev. Code §§ 19.255.005, *et seq.*;
- Whether Defendants' acts and practices constitute negligence;
- Whether Defendants' acts and practices constitute Statutory Larceny through False Pretenses, Cal. Penal Code §§ 484, 496;
- Whether Defendants' acts and practices violated the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d-6;
- Whether Defendants' acts and practices violated Plaintiffs and Class Members' common law privacy rights;
- Whether Defendants breached an express contract;
- Whether Defendants breached an implied contract;
- Whether Defendants' unlawful conduct should be enjoined; and

- Whether damages, restitution, equitable, injunctive, compulsory, or other relief is warranted.

433. Plaintiffs' claims are typical of the claims of the Classes that Plaintiffs seek to represent. As alleged herein, Plaintiffs and the Classes sustained damages arising out of the same unlawful actions and conduct by Defendants.

434. Plaintiffs are willing and prepared to serve the Classes in a representative capacity with all of the obligations and duties material thereto. Plaintiffs will fairly and adequately protect the interests of the Classes and have no interest adverse to or in conflict with, the interests of the other members of the Classes.

435. Plaintiffs' interests are co-extensive with and are not antagonistic to those of absent members within the Classes. Plaintiffs will undertake to represent and protect the interests of absent members within the Classes and will vigorously prosecute this action.

436. Plaintiffs have engaged the services of the undersigned counsel. Counsel is experienced in complex litigation, will adequately prosecute this action, and will assert and protect the rights of, and otherwise represent, Plaintiffs and absent members of the Classes.

437. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiffs know of no difficulty to be encountered in the management of this litigation that would preclude its maintenance as a class action.

438. Class action status is warranted under Federal Rule of Civil Procedure 23(b)(3) because questions of law or fact common to the members of the Classes predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

439. The Classes may also be certified under Federal Rule of Civil Procedure 23(b)(2) because Defendants have acted on grounds generally applicable to the Classes, thereby making it appropriate to award final injunctive relief or corresponding declaratory relief with respect to the Classes.

440. The interest of members within the Classes individually controlling the prosecution of separate actions is theoretical and not practical. The Classes have a high degree of similarity and are cohesive, and Plaintiffs anticipate no difficulty in the management of this matter as a class action.

441. The nature of notice to the proposed Classes is contemplated to be by direct mail and/or email upon certification of the Classes or, if such notice is not practicable, by the best notice practicable under the circumstance including, *inter alia*, email, publication in major newspapers, and/or on the internet.

VII. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Violation of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*
On Behalf of the Kaiser Operating States Class
(Against All Defendants)

442. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

443. Plaintiffs bring this claim individually and on behalf of the Kaiser Operating States Class.

444. The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510, *et seq*., prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication.

445. The ECPA confers a civil cause of action on "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

446. The ECPA protects both the sending and receipt of communications.

447. A violation of the ECPA occurs where any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic communication" or "intentionally discloses, or endeavors to disclose, to any other person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication" or "intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having

reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication." 18 U.S.C. §§ 2511(1)(a), (c)-(d).

448. In addition, "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

449. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

450. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

451. "Contents" includes "any information concerning the substance, purport, or meaning" of the communication at issue. 18 U.S.C. § 2510(8).

452. An "electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

453. Plaintiffs and Kaiser Operating States Class Members' communications with Kaiser Permanente through the Site, Portal, and mobile application are electronic communications under the ECPA.

454. Whenever Plaintiffs and Kaiser Operating States Class Members communicated with Kaiser Permanente and/or their health care providers on the Site or mobile applications, Third Party Wiretappers, through the source code Kaiser embedded and ran on its Site and Apps, contemporaneously and intentionally intercepted, and endeavored to intercept Plaintiffs' and Kaiser Operating States Class Members' electronic communications without authorization or consent.

455. Whenever Plaintiffs and Kaiser Operating States Class Members communicated with Kaiser Permanente and/or their health care providers on the Site or mobile applications, Kaiser, through the source code it imbedded and ran on its Site and Apps, contemporaneously and

intentionally disclosed, and endeavored to disclose the contents of Plaintiffs' and Kaiser Operating States Class Members' electronic communications to the Third Party Wiretappers, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA.

456. Whenever Plaintiffs and Kaiser Operating States Class Members communicated with Kaiser Permanente and/or their health care providers on the Site or mobile applications, Kaiser, through the source code it embedded and ran on the Site and Apps, contemporaneously and intentionally used, and endeavored to use and allow the contents of Plaintiffs and Kaiser Operating States Class Members' electronic communications to be disclosed and used for purposes other than providing health care services to Plaintiffs and Kaiser Operating States Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA.

457. Whenever Plaintiffs and Kaiser Operating States Class Members communicated with Kaiser Permanente and/or their health care providers on the Site or mobile applications, Kaiser, through the source code it embedded and ran on the Site and Apps, contemporaneously and intentionally redirected the contents of Plaintiffs and Kaiser Operating States Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, namely the Third Party Wiretappers.

458. Whenever Plaintiffs and Kaiser Operating States Class Members communicated with Kaiser Permanente and/or their health care providers on the Site or mobile applications, Kaiser, through the source code it embedded and ran on the Site and Apps, contemporaneously and intentionally divulged the contents of Plaintiffs and Kaiser Operating States Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, namely the Third Party Wiretappers.

459. While the ECPA provides that it shall not be unlawful for someone to intercept communications where they are a party, or where one party consents, the ECPA explicitly provides

that this exception does not apply in situations like this where the "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 2511(2)(d).

460. Here, Kaiser Plan Members' communications were intercepted for the purpose of criminally and tortiously using Kaiser Plan Members' identifying information and/or PHI as consideration for Kaiser obtaining Twitter, Google, and Microsoft Bing's technology.

461. While Google, Microsoft Bing, and Twitter do not require monetary payment to use the code that Kaiser installed on the Site and Apps, the implicit cost of this technology is that Kaiser provide Google, Microsoft Bing, and Twitter the ability to use Plaintiffs' and other Kaiser Plan Members' identifying information and/or PHI provided and/or accessed on the Site and/or Apps for better ad targeting. Kaiser thus understood that, in lieu of monetary payments for the use of the Google, Microsoft Bing, and Twitter code, Kaiser would be paying Google, Microsoft Bing, and Twitter in kind by providing them with Plaintiffs and other Kaiser Plan Members' identifying information and/or PHI, which Google, Microsoft Bing, and Twitter could then monetize through marketing. This payment and consideration was not restricted to wiretapping technologies, but pervaded Kaiser's entire approach to marketing.

462. For example, as discovery has now revealed, [redacted] Ex. 8.

463. HHS' guidance for marketing communications states that health care providers may not provide patient lists for marketing purposes without the consent of every included patient:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. **Moreover, covered entities may not sell lists of patients or**

enrollees to third parties without obtaining authorization from each person on the list.[100]

464. Here Kaiser essentially sold its patient lists, and other PHI, to Twitter, Google, and Microsoft Bing without obtaining Kaiser Plan Members' written authorization in exchange for the ability to use Twitter, Google, and Microsoft Bing's technology in violation of the HIPAA Privacy Rule.

465. Kaiser's violation of the HIPAA Privacy Rule is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." *Id*. In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both." *Id.*

466. Kaiser also acted tortiously by using Plaintiffs and other Kaiser Plan Members' personal information without consent or compensation so that Kaiser could obtain Twitter, Google, and Microsoft Bing's market research and consumer analysis technology free of charge, rather than paying for it.

467. Plaintiffs and Kaiser Operating States Class Members did not authorize Kaiser to use their identifying information and/or PHI in order to obtain Twitter, Google, and Microsoft Bing's market research and consumer analysis technology free of charge, rather than paying for it.

468. To be clear, Plaintiffs do not allege that the interception itself was the separate criminal or tortious purpose for the interception; rather, Kaiser's criminal or tortious purpose was to obtain Twitter, Google, and Microsoft Bing's technology at no cost by providing the third parties with Plaintiffs' and other Kaiser Plan Members' identifying information and/or PHI, rather than paying for that technology.

469. Defendants' actions were at all relevant times knowing, willful, and intentional.

470. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Kaiser Operating States Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation

[100] *Marketing* at 1-2, Office for Civil Rights (Rev. Apr. 3, 2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf. (emphasis added).

of the ECPA and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class and any profits made as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

SECOND CLAIM FOR RELIEF
Violation of the California Invasion of Privacy Act
Cal. Penal Code §§ 630, *et seq.*
On Behalf of the Kaiser Operating States Class, or alternatively, On Behalf of the California Sub-Class
(Against Kaiser Foundation Health Plan and Kaiser Foundation Hospitals)

471. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

472. Plaintiffs bring this claim individually and on behalf of the Kaiser Operating States Class, or alternatively, on behalf of the California Sub-Class.

473. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*. ("CIPA"), to address "advances in science and technology [that] 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.

474. Although the "declaration of policy" for CIPA provides that CIPA is intended "to protect the right of privacy of the people of this state," CIPA Section 637.2—titled "Civil action by persons injured; injunction"—provides that an action under CIPA can be brought by "*[a]ny person* who has been injured by a violation of this chapter . . . against the person who committed the violation" Cal. Penal Code § 637.2 (emphasis added). To establish liability under section 631(a), Plaintiffs need only establish that a Defendant, "by means of any machine, instrument, or contrivance, or in any other manner," did any of the following:

> [i] [I]ntentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> Or

> [ii] [W]illfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state,
>
> Or
>
> [iii] [U]ses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> Or
>
> [iv] [A]ids, 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.

475. Under § 631, a defendant must show it had the consent of all parties to a communication.

476. Kaiser Foundation Health Plan and Kaiser Foundation Hospitals and the Third Party Wiretappers are each a "person" for the purposes of CIPA.

477. Kaiser Foundation Health Plan, Inc. and Kaiser Foundation Hospitals maintain their headquarters in California, where they aided, agreed with, employed, and conspired with the Third Party Wiretappers to unlawfully, permit, or cause the Third Party Wiretappers to willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, or attempt to read, or learn the contents or meaning of Kaiser Plan Members' communications while the same were in transit or passing over any wire, line or cable or as being sent from or received at any place within the State of California. Kaiser Foundation Health Plan, Inc. and Kaiser Foundation Hospitals also aided, agreed with, employed, and conspired with the Third Party Wiretappers in the State of California to use, or attempt to use, or communicate information so obtained.

478. Third Party Wiretappers Adobe and Google also maintain their principal places of business in California, where they read, or attempt to read, or learn the contents or meaning of Kaiser Plan Members' communications while the same were in transit or passing over any wire, line, or cable or as being sent from or received at any place within the State of California. These Third Party Wiretappers also, in the State of California, used, use or attempt to use, or communicate information so obtained.

479. The Third Party Wiretappers' code, Plaintiffs and Class Members' browsers, and Plaintiffs and Class Members' computing and mobile devices are all a "machine, instrument, or contrivance, or . . . other manner" used to engaged in the prohibited conduct at issue here. Cal. Penal Code § 631.

480. Kaiser installed the Third Party Wiretappers' code to automatically and secretly spy on, and intercept Plaintiffs and Class Members' communications with Kaiser Permanente through the Site and Apps in real time.

481. At all relevant times, Kaiser's disclosure of Plaintiffs and Class Members' communications to Third Party Wiretappers on the Site and Apps was without Plaintiffs and Class Members' authorization or consent.

482. By installing the Third Party Wiretappers' code on the Site and Apps, Kaiser intentionally caused Plaintiffs and Class Members' communications to be intercepted, recorded, stored, and transmitted to the Third Party Wiretappers.

483. At all relevant times, the Third Party Wiretappers intentionally tapped or made unauthorized connections with, the lines of internet communication between Plaintiffs and Class Members and Kaiser's Site or Apps without the consent of all parties to the communication.

484. The Third Party Wiretappers willfully read or attempt to read or learn the contents or meaning of Plaintiffs and Class Members' communications on Kaiser's Site or mobile applications 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 with Kaiser's Site or Apps in real time.

485. By embedding the Third Party Wiretappers' technology on the Site and Apps, Kaiser aided, agreed with, employed, and conspired with Third Party Wiretappers to carry out the wrongful conduct alleged herein in violation of Cal. Penal Code § 631(a)[iv].

486. As set forth above, Kaiser's embedding the Third Party Wiretappers' code on the Site and Apps posed a materially enhanced risk that Plaintiffs and other Kaiser Plain Members privacy would be compromised.

487. 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.

THIRD CLAIM FOR RELIEF
Common Law Invasion of Privacy—Intrusion Upon Seclusion
On Behalf of the Kaiser Operating States Class, or alternatively, On Behalf of the California Sub-Class, Colorado Sub-Class, District of Columbia Sub-Class, Georgia Sub-Class, Maryland Sub-Class, Oregon Sub-Class, and Washington Sub-Class
(Against All Defendants)

488. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

489. Plaintiffs bring this claim individually and on behalf of the Kaiser Operating States Class, or alternatively, on behalf of the California Sub-Class, Colorado Sub-Class, District of Columbia Sub-Class, Georgia Sub-Class, Maryland Sub-Class, Oregon-Sub-Class, and Washington Sub-Class.

490. Intrusion upon seclusion has occurred when (1) Defendants intruded and/or aided, agreed with, employed, and/or conspired with the Third Party Wiretappers to intrude into a private place, conversation, matter; (2) in a manner that was highly offensive to a reasonable person.

491. Kaiser intentionally intruded upon Plaintiffs and Class Members' solitude or seclusion when it disclosed communications it received from Plaintiffs and Class Members, which was intended to stay private, to Third Party Wiretappers.

492. Plaintiffs and Class Members did not consent to or authorize, nor were they aware of (1) Kaiser's disclosure to Third Party Wiretappers of information that it received from Plaintiffs and Class Members through its Site or Apps or (2) the Third Party Wiretappers' collection of information concerning Plaintiffs and Class Members' activity on the Kaiser Permanente Site or Apps at the time that the disclosure occurred. Plaintiffs and Class Members never agreed that Kaiser could disclose their communications to Third Party Wiretappers, nor did they agree that the Third Party Wiretappers could collect such information.

493. Plaintiffs and Class Members had a reasonable expectation of privacy over their communications with Kaiser, including information obtained from their use of Kaiser's Site, Portal, or Apps.

494. Kaiser knew that by embedding the Third Party Wiretappers' code, they were disclosing and permitting the Third Party Wiretappers to intercept and collect personally identifying, and personal and sensitive information relating to Kaiser Plan Members' medical treatment and/or PHI that Kaiser was required to protect and safeguard. As detailed above, the Third Party Wiretappers' code intercepts, collects, and transmits significant amounts of healthcare-related communications along with personally identifiable information about Kaiser Plan Members, including IP Addresses, first names, marketing IDs, device identifiers and other information that alone or in combination can be used to identify the individual Kaiser Plan Members.

495. Indeed, as Kaiser admitted to regulators in or around April 12, 2024, the "information collected by these technologies about Kaiser members may be considered Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), pursuant to recent guidance from the Department of Health and Human Services (HHS)." However, as set forth above, Kaiser knew that the Third Party Wiretappers' code was intercepting, transmitting, and collecting PHI and other personally identifying information to the Third Party Wiretappers long before the April 12, 2024 disclosure.

496. Kaiser's and the Third Party Wiretappers' intentional intrusion into Plaintiffs and Class Member's communications with Kaiser Permanente, including information obtained from their use of Kaiser's Site or Apps, was highly offensive to a reasonable person in that it violated federal and state criminal and civil laws designed to protect individual privacy.

497. Kaiser's intentional disclosure and collection of private and highly sensitive communications, including information obtained from Plaintiffs and Class Members' use of Kaiser's Site and/or Apps through deceit is highly offensive to a reasonable person. Plaintiffs and Class Members reasonably expected that their communications with Kaiser Permanente, including information obtained from their use of Kaiser's Site or Apps would not be disclosed to third parties.

498. Kaiser's reckless disregard for the privacy of Plaintiffs and the Class Members is highly offensive to a reasonable person. Kaiser knew of the privacy risks posed by the tracking technologies it employed and chose to proceed with the invasion of privacy, as well as deliberately misrepresent its tracking to Plaintiffs and Class Members through inaccurate and/or incomplete disclosures.

499. Secret disclosure and collection of Plaintiffs and Class Members' communications with Kaiser Permanente, including information of millions of individuals obtained from their use of Kaiser's Site or Apps is highly offensive to a reasonable person. 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 information is collected or shared.

500. Plaintiffs and Class Members have suffered harm and injury as a direct and proximate result of Kaiser's invasion of their privacy.

501. Plaintiffs and Class Members are entitled to reasonable compensation, including but not limited to monetary damages.

502. Plaintiffs and Class Members seek appropriate relief for that injury, including, but not limited to injunctive relief and damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as well as a disgorgement of profits earned as a result of its intrusions upon Plaintiffs and Class Members' privacy.

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

FOURTH CLAIM FOR RELIEF
Invasion of Privacy in Violation of the California Constitution, Art. 1, § 1
On Behalf of the Kaiser Operating States Class, or alternatively, On Behalf of the California Sub-Class
(Against Kaiser Foundation Health Plan and Kaiser Foundation Hospitals)

504. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

505. Plaintiffs bring this claim individually and on behalf of the Kaiser Operating States Class, or alternatively, on behalf of the California Sub-Class.

506. Kaiser Foundation Health Plan Inc. and Kaiser Foundation Hospitals are headquartered in California and their conduct took place in California.

507. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Cons. art. I, § 1.

508. The right to privacy in California's constitution creates a right of action against private entities such as Kaiser.

509. To state a California constitutional privacy claim, a plaintiff must establish (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable expectation of privacy; and (3) conduct by the defendant constituting an intrusion of privacy so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

510. Plaintiffs and Class Members possess a legally protected interest in their communications with Kaiser Permanente, including information derived from their use of Kaiser's Site or Apps, and in providing such information to Kaiser Permanent (and receiving information from Kaiser Permanente) without that information being disclosed to Third Party Wiretappers. This legally-protected interest is derived from the common law, the California Constitution's article I, section 1 guarantee of the right to privacy, the ECPA, CIPA, CMIA, and HIPAA.

511. Plaintiffs and Class Members had a reasonable expectation of privacy under the circumstances, including that: (i) the information Kaiser disclosed to Third Party Wiretappers included information related to patient status, health conditions, identifying information, personal and sensitive information, information related to medical treatment, and confidential communications with Kaiser Permanente and its providers; and (ii) Plaintiffs and Class Members did not consent or otherwise authorize Kaiser to disclose this private information and these confidential communications to the Third Party Wiretappers.

512. Defendants' conduct constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the information disclosed by Kaiser and collected by Third Party Wiretappers was highly sensitive and personal, as protected by the California Constitution; (ii) Kaiser did not have authorization or consent to disclose this information to any third party, including Third Party Wiretappers, and the Third Party Wiretappers did not have authorization to collect this

information; and (iii) the invasion deprived Plaintiffs and Class Members the ability to control the circulation of said information, which is considered a fundamental right to privacy.

513. Defendants' invasion violated the privacy rights of millions of Class Members, including Plaintiffs, without authorization or consent. Their conduct constitutes a severe and egregious breach of social norms.

514. As a direct and proximate result of Defendants' actions, Plaintiffs and Class Members have had their privacy invaded and sustained damages and will continue to suffer damages.

515. Plaintiffs and Class Members seek appropriate relief for that injury, including but not limited to injunctive relief and damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as well as a disgorgement of profits earned as a result of their intrusions upon Plaintiffs and Class Members' privacy.

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

FIFTH CLAIM FOR RELIEF
Breach of Express Contract
On Behalf of the Kaiser Operating States Breach of Contract Sub-Class or alternatively, On Behalf of the California Breach of Contract Sub-Class, the Colorado Breach of Contract Sub-Class, the District of Columbia Breach of Contract Sub-Class, the Georgia Breach of Contract Sub-Class, the Maryland Breach of Contract Sub-Class, the Oregon Breach of Contract Sub-Class, the Virginia Breach of Contract Sub-Class, and the Washington Breach of Contract Sub-Class
(Against Kaiser Foundation Health Plan)

517. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

518. Plaintiffs bring this claim individually and on behalf of the Kaiser Operating States Breach of Contract Sub-Class, or alternatively, on behalf of the California Breach of Contract Sub-Class, Colorado Breach of Contract Sub-Class, the District of Columbia Breach of Contract Sub-Class, the Georgia Breach of Contract Sub-Class, the Maryland Breach of Contract Sub-Class, the Oregon Breach of Contract Sub-Class, the Virginia Breach of Contract Sub-Class, and the Washington Breach of Contract Sub-Class.

519. There exists an express contract between Plaintiffs and the Breach of Contract Sub-Class Members on the one side, and Kaiser Foundation Health Plan on the other, when Plaintiffs and Breach of Contract Sub-Class Members shared and/or accessed information on the Kaiser Portal or

Apps, namely the Terms & Conditions and Privacy Statement for the Kaiser website (hereinafter referred to as the "express contract" or "Terms and Conditions"). A true and correct copy of the Terms and Conditions[101] last updated June 2022, is attached hereto as Exhibit 4, and a copy of the Privacy Statement, incorporated into the Terms and Conditions, is attached as Exhibit 5.

520. Specifically, at the bottom of the Portal Login Page, Kaiser Foundation Health Plan agrees, contracts, and warrants that: "By signing in, you agree to our website Terms & Conditions and Privacy Statement." https://healthy.kaiserpermanente.org/southern-california/register (last visited Dec. 5, 2024). The relevant app store pages for the Kaiser Permanente App and Kaiser Permanente Washington App also provide that use of each app is governed by Kaiser Terms & Conditions and the Kaiser Privacy Statement. To access their medical information on the Portal and Apps, Kaiser Foundation Health Plan expressly requires that Kaiser Plan Members agree to the Terms and Conditions.

521. To access information in the Portal and on the Kaiser Permanente App, John Doe clicked buttons signifying acceptance of Kaiser's Terms and Conditions (including the incorporated Privacy Statement) and thus entered into a contract with Kaiser Foundation Health Plan regarding use of the Site and Kaiser Permanente App.

522. To access information in the Portal and on the Kaiser Permanente App, John Doe II clicked buttons signifying acceptance of Kaiser's Terms and Conditions (including the incorporated Privacy Statement) and thus entered into a contract with Kaiser Foundation Health Plan regarding use of the Site and Kaiser Permanente App.

523. To access information in the Portal and on the Kaiser Permanente App, John Doe III clicked buttons signifying acceptance of Kaiser's Terms and Conditions (including the incorporated Privacy Statement) and thus entered into a contract with Kaiser Foundation Health Plan regarding use of the Site and Kaiser Permanente App.

524. To access information in the Portal and on the Kaiser Permanente Washington App, Jane Doe clicked buttons signifying acceptance of Kaiser's Terms and Conditions (including the

[101] The Terms and Conditions are materially identical for all Kaiser Regions.

incorporated Privacy Statement) and thus entered into a contract with Kaiser Foundation Health Plan regarding use of the Site and Kaiser Permanente Washington App.

525. To access information in the Portal and on the Kaiser Permanente App, Jane Doe II clicked buttons signifying acceptance of Kaiser's Terms and Conditions (including the incorporated Privacy Statement) and thus entered into a contract with Kaiser Foundation Health Plan regarding use of the Site and Kaiser Permanente App.

526. To access information in the Portal and on the Kaiser Permanente App, Jane Doe III clicked buttons signifying acceptance of Kaiser's Terms and Conditions (including the incorporated Privacy Statement) and thus entered into a contract with Kaiser Foundation Health Plan regarding use of the Site and Kaiser Permanente App.

527. To access information in the Portal and on the Kaiser Permanente App, Jane Doe IV clicked buttons signifying acceptance of Kaiser's Terms and Conditions (including the incorporated Privacy Statement) and thus entered into a contract with Kaiser Foundation Health Plan regarding use of the Site and Kaiser Permanente App.

528. To access information in the Portal and on the Kaiser Permanente App, Jane Doe V clicked buttons signifying acceptance of Kaiser's Terms and Conditions (including the incorporated Privacy Statement) and thus entered into a contract with Kaiser Foundation Health Plan regarding use of the Site and Kaiser Permanente App.

529. To access information in the Portal and on the Kaiser Permanente App, Alexis Sutter clicked buttons signifying acceptance of Kaiser's Terms and Conditions (including the incorporated Privacy Statement) and thus entered into a contract with Kaiser Foundation Health Plan regarding use of the Site and Kaiser Permanente App.

530. By signing into the Portal and/or signing into the Apps, all other Kaiser Plan Members similarly entered into an express contract with Kaiser Foundation Health Plan regarding their respective rights and responsibilities with respect to the Site and Apps.

531. The Kaiser Terms & Conditions, available via hyperlink, further provide: "Any personal information you submit to the Site (for yourself or someone else) is governed by our Website and KP Mobile Application Privacy Statement." S*ee* Ex. 4.

532. The Privacy Statement provides repeated promises that the privacy of Users' personal information will be protected. Indeed, the Kaiser Permanente Privacy Statement at the outset assures Users that "Kaiser Permanente is committed to protecting the privacy of the users of the Site. We will use and disclose your personal information as stated in this Privacy Statement." *See* Ex. 5.

533. However, nowhere does the Privacy Statement disclose that Kaiser embedded code on the Site and Apps which intercept Users and Kaiser Plan Members' communications while they are in transit and commands Users' browsers to send the GET requests and POST transmissions that include personally identifiable information, and healthcare information, including PHI, to the Third Party Wiretappers. The Privacy Statement also does not disclose that all of Users' interactions with the Site and Apps are being intercepted, transmitted and recorded by Session Reply providers such as Quantum Metric and Dynatrace.

534. In the Privacy Statement, Kaiser Foundation Health Plan also agrees, contracts, and warrants that Kaiser's data collection will conform to those requirements imposed by state and federal law, and additionally promises not to "sell or rent personal information about visitors to the Site." *See* Ex. 5.

535. However, Kaiser Foundation Health Plan materially breached these terms by disclosing Plaintiffs and Breach of Contract Sub-Class Members' personally identifying information and PHI to Third Party Wiretappers. Additionally, as detailed above, part of the implicit cost of receiving Google, Microsoft Bing, and Twitter's software is the ability to allow these entities to use the information received to supplement user profiles for better targeting and bolster their ad networks. Kaiser thus understood that, in lieu of monetary payments for the use of those Third Party Wiretappers' code, Kaiser would be paying these entities in kind by providing them with personally identifying information and PHI from Kaiser Health Plan members that those Third Party Wiretappers could then monetize. This exchange between Kaiser and the Third Party Wiretappers amounted to Kaiser selling Plaintiffs' and Breach of Contract Sub-Class Members personally identifiable information in breach of its promise not to do so under the Privacy Statement.

536. In the Privacy Statement, Kaiser Foundation Health Plan further agrees, contracts, and warrants that User data is collected on an aggregate basis, that information is only used to improve

Kaiser's content and overall usage, and that this data is not shared with other organizations for their independent use:

> In addition to web logs . . . ***Kaiser Permanente routinely gathers data*** on Site activity, such as how many people visit the Site, the web pages or mobile screens they visit, where they come from, how long they stay, etc. ***The data is collected on an aggregate basis, which means that no personally identifiable information is associated with the data.*** This data ***helps us improve our content and overall usage.*** The information ***is not shared with other organizations*** for their independent use.[102]

537. However, this statement was false and misleading for multiple reasons, including because, as described above: (1) it is not just Kaiser that is routinely gathering data on Site activity, but also the Third Party Wiretappers; (2) the data was not collected on an aggregate basis, but instead included personally identifiable information associated with that data; (3) Kaiser's data collection was not just for improving content and overall usage but was also for targeted marketing; and (4) this data was shared with other organizations for their independent use.

538. In the Privacy Statement, Kaiser Foundation Health Plan also agrees, contracts, and warrants that the internet "cookies" and "similar technologies" deployed on the Site and Apps will not contain information about Plaintiffs' or Class Members' health history or other personal health information:

> We and our service providers may place Internet "cookies" ***or similar technologies*** (JavaScript, HTML5, ETag) on the computer hard drives of visitors to the Site. Information we obtain helps us to tailor our Site to be more helpful and efficient for our visitors. For example, we are able to see the navigation path taken by users, and that information allows us to understand user success or challenges with the web experience. ***The cookie consists of a unique identifier that does not contain information about your health history.*** We use two types of cookies, "session" cookies and "persistent" cookies, along with ***other similar technologies***.[103]

539. Kaiser Foundation Health Plan further agrees, contracts, and warrants that it will not collect or link personal health information with a "web beacon":

> We may also occasionally use "Web beacons" (also known as "clear gifs," "Web bugs," "1-pixel gifs," etc.) that allow us to collect ***non-personal information*** about your response to our email communications, and for other purposes. Web beacons are tiny images, placed on a Web page or email, that can tell us if you've gone to a particular area on our Site. For example, if you've given us permission to send you emails, we may send you an email urging you to use a certain feature on our Site. If you do respond to that email and use that feature, the Web beacon will tell us that our email communication with you has been successful. ***We do not collect any***

[102] Ex. 5.
[103] *Id.*

> ***personal health information with a Web beacon, and do not link Web beacons with any other personal health information you've given us.***
>
> Since ***Web beacons are used in conjunction with persistent cookies*** (described above), if you set your browser to decline or deactivate cookies, Web beacons cannot function.
>
> Our mobile application contains software development kits (SDKs) that may collect and transmit information back to us or third party partners about your usage of that mobile application or other applications on your device. ***Such data, when collected by a 3rd party, that may show what click path was taken, what pages users visited and how long certain pages took to display, is not identifiable to you as an individual.***[104]

540. However, these statements were false and misleading because Kaiser Foundation Health Plan did not disclose that the "cookies" and "web beacons" would be transmitted in and along with GET requests and POSTs which, as detailed above, did transmit individually identifiable personal information, and PHI, to the Third Party Wiretappers. Indeed, as Kaiser has now represented in filings with state and federal regulators, Kaiser's use of "online technologies (sometimes called 'cookies' or 'pixels')" resulted in the disclosure of "information about Kaiser members" which "may be considered Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA)," including their "IP address, name, information that could indicate a member was signed into a Kaiser Permanente account or service, information showing how the member interacted with and navigated through the website or mobile applications, and search terms used in the health encyclopedia."[105] The Privacy Statement also does not disclose or describe Kaiser's use of the "cookie synching" technology described above.

541. In the Privacy Statement, Kaiser Foundation Health Plan also agrees, contracts, and warrants that any disclosures of personal information by its vendors or contractors will be in compliance with applicable law, and any use of the data by third-parties will be pursuant to Kaiser's written instructions:

> We may disclose personal information to any person performing audit, legal, operational, or other services for us. ***We will use information which does not identify the individual*** for these activities whenever reasonably possible. ***Information disclosed to vendors or contractors*** for operational purposes ***may not be re-disclosed*** to others by such a vendor or contractor, ***except as permitted by KP and applicable law***.

---

[104] *Id.*
[105] Notice at Ex. A, ECF No. 127-1.

> We may also disclose your personal information to third parties who provide services on our behalf to help with our business activities. ***These companies are authorized to use your personal information only as necessary to provide these services to us pursuant to written instructions.*** In such cases, these companies must abide by our data privacy and security requirements, and are not allowed to use your personal information they receive from us for any other purpose.[106]

542. However, Kaiser Foundation Health Plan also materially breached this term by installing the Third Party Wiretappers' code on the Site and Apps by providing personally identifiable information to the Third Party Wiretappers and failing to take sufficient measures to ensure that certain Third Party Wiretappers would only use Kaiser Plan Members' personal information as necessary to provide services for Kaiser. Moreover, Kaiser ***did not provide written instructions*** to some or all of the Third Party Wiretappers detailing how the Third Party Wiretappers are authorized to use Kaiser Plan Members' personal information. At a minimum, this failure materially enhanced the risk that Kaiser Plan Members' personally identifiable information, PHI, and other confidential information would be exposed and/or used without their authorization or consent.

543. Despite its assurances of privacy and confidentiality, Kaiser intentionally incorporated the Third Party Wiretappers' code and recording technology on the Kaiser Site, Portal, and mobile applications, disclosing the contents of Plaintiffs and Breach of Contract Sub-Class Members' information and confidential communications with Kaiser and its providers to Third Party Wiretappers, including for advertising purposes.

544. In exchange for Kaiser Foundation Health Plan's provision of a secure website, patient Portal, and mobile applications, Plaintiffs and Breach of Contract Sub-Class Members were able to make appointments, view medical history, get test results, and find and communicate with doctors, among other things, by way of the patient Portal, instead of doing so by other means, such as by phone or in person.

Consent

545. Kaiser Foundation Health Plan requires Kaiser Plan Members to consent to the Site Terms and Conditions in the process of signing up for, and using, the patient Portal or mobile applications.

[106] Ex. 5.

546. Plaintiffs and Breach of Contract Sub-Class Members consented to the Site Terms and Conditions by signing up for, and using, the Kaiser patient Portal or mobile applications.

Consideration

547. The Kaiser patient Portal and mobile applications are not services Kaiser provides without receiving anything from Plaintiffs and Breach of Contract Sub-Class Members in return. To the contrary, Plaintiffs and Breach of Contract Sub-Class Members' use of the patient Portal and mobile applications confers significant benefit upon Kaiser Foundation Health Plan—a benefit to which Kaiser Foundation Health Plan is not entitled—including, but not limited to, increased efficiency, optimized workflow, cost reduction, and receipt of incentive payments from the federal government (HHS) via the Meaningful Use Program. As just one example, Breach of Contract Sub-Class Members use of the patient Portal and mobile applications to access test results and make appointments results in Kaiser Permanente being freed up from performing such tasks of scheduling and reporting on test results for patients, thereby cutting down on long phone calls or in-office communications, increasing efficiency and decreasing costs.

548. In fact, according to a blog post on the health policy website, Health Affairs,[107] Kaiser offers "the largest private-sector patient portal in the U.S.," which "help[s] our health care system improve outcomes and manage resources." The Portal has led to a "2 to 6.5 percent improvement in Healthcare Effectiveness Data and Information Set (HEDIS) performance measures," improved patient loyalty by making portal uses "2.6 times more likely to remain Kaiser Permanente members," and shifted patient interactions from in-person to secure messenger.

549. Thus, Kaiser Foundation Health Plan benefits from Breach of Contract Sub-Class Members' use of their online Portal and mobile applications by: (1) making their provision of healthcare services more efficient, and (2) reducing the costs associated with managing their members' medical conditions. Importantly, as an integrated managed care consortium, Kaiser Permanente is both a healthcare provider and insurer—thus, Kaiser Foundation Health Plan is in a position to realize any savings generated by reducing patient costs.

[107] Terhilda Garrido, Brian Raymond, & Ben Wheatley, *Lessons From More Than A Decade In Patient Portals*, Health Affairs (Apr. 7, 2016), https://www.healthaffairs.org/do/10.1377/forefront.20160407.054362.

550. Additionally, Plaintiffs and Breach of Contract Sub-Class Members agree to the Terms and Conditions when using the Site and/or App. In fact, the Terms and Conditions explicitly provide that:

> BY USING THE SITE OR BY CLICKING "I ACCEPT" BELOW, YOU SIGNIFY YOUR AGREEMENT TO THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, DO NOT USE THE SITE.[108]

551. The Terms and Conditions are also presented via hyperlink just below the "Sign In" fields required to be completed in order to access the purportedly secure patient Portal on the Site and Apps, with a notification just below the "Sign In" fields that provides: "By signing in, you agree to our website Terms & Conditions and Privacy Statement."

552. Agreeing to the Terms and Conditions is additional consideration that Plaintiffs and Breach of Contract Sub-Class Members provide to Kaiser in exchange for Kaiser permitting them to use the Site and the Apps and Kaiser's promises made to Users in the Privacy Statement.

553. Ultimately, under the Terms and Conditions, Plaintiffs and Breach of Contract Sub-Class Members agree to share their personally identifiable information while using the Site and Apps, conferring a significant benefit on Kaiser beyond what Kaiser was entitled pursuant to the terms of the Evidence of Coverage, in exchange for Kaiser's agreement to abide by it promises set forth in the Terms and Conditions for how that personally identifiable information will be used.

554. Accordingly, Plaintiffs and Breach of Contract Sub-Class Members provided Kaiser with unique consideration explicitly tied to use of the Site and Apps.

Performance

555. Plaintiffs and Breach of Contract Sub-Class Members performed under the express contract.

Kaiser Foundation Health Plan's Breach of the Express Contract

556. Kaiser Foundation Health Plan materially breached its express contract with Plaintiffs and Breach of Contract Sub-Class Members by disclosing to the Third Party Wiretappers, Plaintiffs and Breach of Contract Sub-Class Members' patient status, personally identifiable data, and confidential communications with Kaiser Permanente, thereby failing to provide Plaintiffs and

[108] Ex. 4.

Breach of Contract Sub-Class Members with the secure method of communication it agreed to provide.

557. The patient health information Kaiser Foundation Health Plan used and disclosed to unauthorized third parties includes:

a. Breach of Contract Sub-Class Members' IP addresses, User-Agent data, persistent cookie identifiers, device identifiers, and/or browser fingerprint information—all of which constitute personally identifiable data both alone and in combination with other data;

b. the date and time of Breach of Contract Sub-Class Members' registration for the Portal;

c. the date and time of every Breach of Contract Sub-Class Members' sign-in and logoff of the "secure" the Portal and mobile applications;

d. the contents of communications Breach of Contract Sub-Class Members' exchange inside the "secure" Portal and mobile applications;

e. the contents of communications Breach of Contract Sub-Class Members' exchange after they have logged off the Portal;

f. the contents of communications Breach of Contract Sub-Class Members' exchange with Kaiser Permanente seeking providers who accept specific insurance products while still signed in to the "secure" Portal and mobile applications; and

g. all other HTTPS communications patients exchange with Kaiser Permanente and its providers on the Site and mobile applications that Kaiser has permitted the third parties to correlate with the patient's status as a patient, and the particular dates and times for which they access the "secure" Portal and mobile applications.

558. Indeed, Kaiser has admitted in filings with state and federal regulators that there has been "unauthorized access to certain limited personal information stemming from Kaiser's prior use of certain third party online technologies on its website and mobile application," including Plaintiffs' and Class Members' "IP address, name, information that could indicate a member was signed into a Kaiser Permanente account or service, information showing how the member interacted with and navigated through the website or mobile applications, and search terms used in the health encyclopedia."[109]

559. As detailed above, Kaiser's installation of the Third Party Wiretappers' code on the Site and Apps was contrary to the provisions of the Privacy Statement, and constitutes a breach of Plaintiffs' and Class Members' express contract with Kaiser.

[109] Notice at Ex. A, ECF No. 127-1.

560. The patient data Kaiser discloses (Plaintiffs and Breach of Contract Sub-Class Members' patient status, personally identifiable data, and confidential communications with Kaiser Permanente and its providers) is not aggregated as specified in the Privacy Statement.

561. Nevertheless, information that Plaintiffs and Breach of Contract Sub-Class Members reasonably thought was being transmitted "securely" to Kaiser Permanente was being disclosed by Kaiser to unauthorized third parties as follows:

a. A Kaiser Plan Member signs in to the "secure" patient Portal and mobile applications;

b. On sign-in, Kaiser discloses the fact of the sign in to the Third Party Wiretappers;

c. Once signed-in, if a Kaiser Plan Member clicked to, for example:

i. view tests, a disclosure of that action was made to the Third Party Wiretappers of the specific tests; or,

ii. Find-A-Doctor, or set an appointment, a disclosure of that action was made to Third Party Wiretappers.

iii. The above examples of patient communications about the doctor or the appointment was shared with Third Party Wiretappers while the Kaiser Plan Member was still logged-in to the "secure" patient Portal or mobile application; and

d. On logoff, Kaiser discloses this action to the Third Party Wiretappers.

562. Kaiser Foundation Health Plan failed to cure these breaches and continued to disclose to Third Party Wiretappers Plaintiffs and Breach of Contract Sub-Class Members' personally identifiable data and communications with Kaiser Permanente until at least November 2023.

Plaintiffs and Breach of Contract Sub-Class Members Were Damaged

563. Kaiser Foundation Health Plan's breach caused Plaintiffs and Breach of Contract Sub-Class Members the following damages, among others:

a. Nominal damages for each breach of contract by Defendants;

b. General damages for invasion of their rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Sensitive and confidential information that Plaintiffs and Breach of Contract Sub-Class Members intended to remain private is no longer private;

d. Defendants eroded the essential confidential nature of the provider-patient relationship;

e. Defendants took something of value from Plaintiffs and Breach of Contract Sub-Class Members and derived a benefit therefrom without Plaintiffs and Breach of Contract Sub-Class Members' knowledge or informed consent and without sharing the benefit of such value;

f. Plaintiffs and Breach of Contract Sub-Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to maintain confidentiality;

g. Defendants' actions diminished the value of Plaintiffs and Breach of Contract Sub-Class Members' personal information;

h. Defendants' actions violated the property rights that Plaintiffs and Breach of Contract Sub-Class Member enjoy in their private communications; and

i. Defendants' actions violated the property rights that Plaintiffs and Breach of Contract Sub-Class Members enjoy in their personally identifiable medical data and communication.

564. Plaintiffs and Breach of Contract Sub-Class Members also seek attorney's fees and costs on this claim to the extent allowable.

SIXTH CLAIM FOR RELIEF
Breach of Implied Contract
Pled in the Alternative to Express Breach of Contract
On Behalf of the Kaiser Operating States Breach of Contract Sub-Class, or Alternatively, On Behalf of the California Breach of Contract Sub-Class, the Colorado Breach of Contract Sub-Class, the District of Columbia Breach of Contract Sub-Class, the Georgia Breach of Contract Sub-Class, the Maryland Breach of Contract Sub-Class, the Oregon Breach of Contract Sub-Class, the Virginia Breach of Contract Sub-Class, and the Washington Breach of Contract Sub-Class
(Against All Defendants)

565. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

566. Plaintiffs bring this claim on behalf of themselves and the Kaiser Operating States Breach of Contract Sub-Class, or alternatively on behalf of the California Breach of Contract Sub-Class, Colorado Breach of Contract Sub-Class, the District of Columbia Breach of Contract Sub-Class, the Georgia Breach of Contract Sub-Class, the Maryland Breach of Contract Sub-Class, the Oregon Breach of Contract Sub-Class, the Virginia Breach of Contract Sub-Class, and the Washington Breach of Contract Sub-Class.

567. An implied contract was created between Kaiser, on the one side, and Plaintiffs and Breach of Contract Sub-Class Members, on the other hand, whereby Kaiser offered to provide Plaintiffs and Breach of Contract Sub-Class Members what it represented to be a secure Portal and secure mobile applications through which Plaintiffs and Breach of Contract Sub-Class Members could confidentially make appointments, review medical history, get test results, communicate with providers, and find doctors, among other things, and Plaintiffs and Breach of Contract Sub-Class

Members agreed to use the purportedly secure Portal and mobile applications to make appointments, view medical history, get test results, and find and communicate with doctors, among other things, instead of doing so by other means, such as by phone or in person.

Mutual Assent

568. Such implied contract was created by virtue of the relationship and conduct of the parties, as well as the surrounding circumstances, including, but not limited to:

a. The confidential nature of the medical-provider/patient relationship between Kaiser Permanente and Plaintiffs and Breach of Contract Sub-Class Members;

b. Kaiser Foundation Health Plan's express promises, as noted above, to maintain the privacy and confidentiality of patients' personally identifiable data and communications that Plaintiffs and Breach of Contract Sub-Class Members exchange with Kaiser Permanente at the Site and mobile applications;

c. Kaiser's creation of purportedly secure patient Portal and mobile applications that requires a sign-in with a user name and password, which would lead a reasonable person to believe that their communications with Kaiser Permanente while signed in to the Portal would not be shared outside of Kaiser; and

d. Plaintiffs and Breach of Contract Sub-Class Members' use of the purportedly secure Portal and mobile applications to make appointments, get test results, and find doctors, among other things, instead of doing so by other means, such as by phone or in person.

569. Kaiser knew, or had reason to know, that Plaintiffs and Breach of Contract Sub-Class Members would interpret the parties' relationship and conduct as an agreement to keep Plaintiffs and Breach of Contract Sub-Class Members' patient status, personally identifiable data, and communications with Kaiser Permanente inside the Portal and mobile applications confidential when Plaintiffs and Breach of Contract Sub-Class Members used Kaiser's patient Portal and mobile applications.

Consideration

570. The patient Portal and mobile applications are not services Kaiser Permanente provides without receiving anything from Plaintiffs and other patients in return. To the contrary, Plaintiffs and Breach of Contract Sub-Class Members' use of the Portal and mobile applications confers significant benefit upon Kaiser—a benefit to which Kaiser is not entitled—including, but not limited to, increased efficiency, optimized workflow, cost reduction, and receipt of incentive payments from the federal government (United States Department of Health and Human Services) via the Meaningful Use Program.

571. As just one example, patients' use of the patient Portal and mobile applications to access test results and make appointments results in Kaiser being freed up from performing such tasks of scheduling and reporting on test results for patients, thereby cutting down on long phone calls or in-office communications, increasing efficiency and decreasing costs.

572. As a result, and as further noted above, Kaiser is able to more efficiently allocate resources and benefits from improved—and, thus, less costly—patient outcomes and increased patient loyalty.

Performance

573. Plaintiffs and Breach of Contract Sub-Class Members performed under the implied contract.

Kaiser's Breach of the Implied Contract

574. Kaiser materially breached its implied contract with Plaintiffs and Breach of Contract Sub-Class Members, by disclosing to third party companies, Plaintiffs and Breach of Contract Sub-Class Members' patient status, personally identifiable data, and confidential communications with Kaiser Permanente made within the patient Portal and mobile applications, thereby failing to provide Plaintiffs and Class Members with the secure site and mobile applications it agreed to provide.

575. The patient health information Kaiser used and disclosed to unauthorized third parties for marketing includes:

a. Breach of Contract Sub-Class Members' IP addresses, User-Agent data, persistent cookie identifiers, device identifiers, and/or browser fingerprint information—all of which constitute personally identifiable data both alone and in combination with other data;

b. the date and time of Breach of Contract Sub-Class Members' registration for the Portal;

c. the date and time of every Breach of Contract Sub-Class Member's sign-in and logoff of the "secure" Portal and mobile applications;

d. the contents of communications Breach of Contract Sub-Class Members exchange inside the "secure" Portal and mobile applications;

e. the contents of communications Breach of Contract Sub-Class Members exchange after they have logged off the Portal and mobile applications;

f. the contents of communications Breach of Contract Sub-Class Members exchange with Kaiser Permanente seeking providers who accept specific insurance products while still signed in to the "secure" Portal and mobile applications; and

g. all other HTTPS communications patients exchange with Kaiser Permanente at the Site that Kaiser has permitted the third parties to correlate with the Breach of Contract Sub-Class Members' status as a patient and the particular dates and times for which they access the "secure" Portal and mobile applications.

576. Indeed, Kaiser has admitted in filings with state and federal regulators that there has been "unauthorized access to certain limited personal information stemming from Kaiser's prior use of certain third party online technologies on its website and mobile application," including Plaintiffs' and Class Members' "IP address, name, information that could indicate a member was signed into a Kaiser Permanente account or service, information showing how the member interacted with and navigated through the website or mobile applications, and search terms used in the health encyclopedia."[110]

577. The patient data Kaiser discloses (Plaintiffs and Breach of Contract Sub-Class Members patient status, personally identifiable data, and confidential communications with Kaiser Permanente and its providers) is not aggregated as specified in the Privacy Statement.

578. Nevertheless, information that Plaintiffs and Breach of Contract Sub-Class Members reasonably thought was being transmitted "securely" to Kaiser Permanente within the patient Portal and mobile applications was being disclosed by Kaiser to unauthorized third parties as follows:

a. A patient signs in to the "secure" patient Portal and mobile applications;

b. On sign-in, Kaiser Permanente discloses the fact of the sign in to the Third Party Wiretappers;

c. Once signed-in, if a patient clicked to, for example:

i. view tests, a disclosure of that action was made to the Third Party Wiretappers of the specific tests; or,

ii. Find-A-Doctor, or set an appointment, a disclosure of that action was made to the Third Party Wiretappers;

iii. The above examples of patient communications about the doctor or the appointment was shared with the Third Party Wiretappers while the patient was still logged-in to the "secure" patient Portal and mobile applications; and

d. On logoff, Kaiser discloses this action to the Third Party Wiretappers.

579. Kaiser failed and refused to cure these breaches and continued to disclose to unauthorized third parties Plaintiffs' and Breach of Contract Sub-Class Members' patient status,

[110] Notice at Ex. A, ECF No. 127-1.

personally identifiable data, and communications with Kaiser Permanente and its providers exchanged on the Site, Portal, and mobile applications until at least November 2023.

Plaintiffs and Breach of Contract Sub-Class Members Were Damaged

580. Defendants' breach caused Plaintiffs and Breach of Contract Sub-Class Members the following damages, among others:

a. Nominal damages for each breach of contract by Defendants;

b. General damages for invasion of their rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Sensitive and confidential information that Plaintiffs and Breach of Contract Sub-Class Members intended to remain private is no longer private;

d. Defendants eroded the essential confidential nature of the provider-patient relationship;

e. Defendants took something of value from Plaintiffs and Breach of Contract Sub-Class Members and derived benefit therefrom without Plaintiffs and Breach of Contract Sub-Class Members' knowledge· or informed consent and without sharing the benefit of such value;

f. Plaintiffs and Breach of Contract Sub-Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to maintain confidentiality;

g. Defendants' actions diminished the value of Plaintiffs and Breach of Contract Sub-Class Members' personal information;

h. Defendants' actions violated the property rights Plaintiffs and Breach of Contract Sub-Class Members enjoy in their private communications; and

i. Defendants' actions violated the property rights Plaintiffs and Breach of Contract Sub-Class Members enjoy in their personally identifiable medical data and communication.

581. Plaintiffs and Breach of Contract Sub-Class Members also seek attorneys' fees and costs on this claim to the extent allowable.

SEVENTH CLAIM FOR RELIEF
Negligence (Including Negligence Per Se)
On Behalf of the Kaiser Operating States Class, or alternatively, On Behalf of the California Sub-Class, Colorado Sub-Class, District of Columbia Sub-Class, Georgia Sub-Class, Maryland Sub-Class, Oregon-Sub-Class, Virginia Sub-Class, and Washington Sub-Class (Against All Defendants)

582. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

583. Plaintiffs bring this claim individually and on behalf of the Kaiser Operating States Class, or alternatively, on behalf of the California Sub-Class, Colorado Sub-Class, District of

Columbia Sub-Class, Georgia Sub-Class, Maryland Sub-Class, Oregon-Sub-Class, Virginia Sub-Class, and Washington Sub-Class.

584. At all times, Kaiser had an obligation to comply with all applicable statutes, including ECPA and HIPAA, as well as state laws governing: wiretapping, computer crimes, insurance information, medical and health information, and larceny.

585. Pursuant to state wiretapping laws—specifically, the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*, the Maryland Wiretap Act, Md. Code Ann., Cts. & Jud. Proc. § 10-401, and the Washington Privacy Act, Wash. Rev. Code §§ 9.73, *et seq.*—Kaiser was prohibited from unlawfully intercepting, disclosing, or using Plaintiffs' and Class Members' electronic communications.

586. Pursuant to state computer crime statutes—specifically, the Georgia Computer Systems Protection Act, Ga. Code Ann. § 16-9-93, and the Virginia Computer Crimes Act, Va. Code Ann. §§ 18.2-152.1, *et seq.*—Kaiser was prohibited from, *inter alia*, using computers or computer networks for the unauthorized, fraudulent, or deceitful copy, collection, taking, appropriation, or conversion of computer data or property.

587. Pursuant to state insurance information statutes—specifically, the Georgia Insurance and Information Privacy Act, Ga. Code Ann. §§ 33-39-1, *et seq.*, and the Virginia Insurance Information and Privacy Protection Act, Va. Code Ann. § 38.2-600, *et seq.*—Kaiser was prohibited from disclosing Plaintiffs' and Class Members' personal or privileged information without authorization.

588. Pursuant to state medical and health information statutes—specifically the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.10, the Virginia Breach of Medical Information Notification Act, Va. Code § 32.1-127.1:05, and the Washington Health Care Information Act, Wash. Rev. Code §§ 70.02.005, *et seq.*—Kaiser was prohibited from disclosing Plaintiffs' and Class Members' medical information without authorization.

589. Pursuant to state data breach notification statutes—specifically the California Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, the Colorado Notification of Security Breach, Colo. Rev. Stat. § 6-1-716, the District of Columbia Consumer Personal Information Security

Breach Notification Act, D.C. Code §§ 28-3851, *et seq*., the Georgia Security Breach of Computerized Information Act. Ga. Code §§ 10-1-910, *et seq*., the Hawaii Security Breach of Personal Information Act, Haw. Rev. Stat. §§ 487N-1, *et seq*., the Maryland Personal Information Protection Act. Md. Code Ann. Com. Law §§ 14-3501 *et seq*., the Oregon Consumer Information Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq*., the Virginia Breach of Personal Information Notification, Va. Code § 18.2-186.6, and the Washington Personal Information—Notice of Security Breaches, Wash. Rev. Code § 19.255.010—Kaiser was required to provide timely notification, no later than thirty or forty-five days under certain statutes, to Plaintiffs and Class Members, the state attorney general, the state consumer protection office, the state health commissioner, and/or consumer reporting agencies when Plaintiffs' and Class Members' personal information was accessed and/or acquired without authorization.

590. Pursuant to California's Larceny statute, Cal. Penal Code §§ 484, 496, Kaiser was prohibited from obtaining Plaintiffs' and Class Members' private health information in a manner constituting theft.

591. Plaintiffs and Class Members are within the class of persons that these statutes are intended to protect.

592. Plaintiffs' and Class Members' injuries are the type of harm that these statutes are intended to prevent.

593. Defendants' failure to comply with the above statutes constitutes negligence *per se*.

594. Additionally, by intercepting and/or aiding, agreeing, employing, and/or conspiring with, third parties that are intercepting and recording the private information that Kaiser Plan Members are sending, accessing, reviewing, or receiving through the Site, Portal, and Apps, Kaiser acted in a way that a reasonable person should recognize as involving an unreasonable risk of invading the interest of another. Specifically, Kaiser knew or should have known that the disclosure of Plaintiffs' and Class Members' personally identifiably information would compromise the privacy of Plaintiffs and Class Members and put the security of their personally identifiable information at risk.

595. Kaiser knowingly collected the personally identifiable information of Plaintiff and Class Members and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being disclosed to third parties including the Third Party Wiretappers.

596. Plaintiffs and Class Members entrusted their personally identifiable information, including PHI, to Kaiser in order to use the Site and Apps and Kaiser owed Plaintiffs and Class Members a duty to take reasonable steps to prevent the disclosure of their personally identifiable information to the Third Party Wiretappers.

597. Moreover, by intercepting and/or aiding, agreeing, employing, and/or conspiring with, third parties that are intercepting and recording the private information that Kaiser Plan Members are sending, accessing, reviewing, or receiving through the Site, Portal, and Apps – or failing to exercise due care and take adequate steps to safeguard Kaiser Plan Members' personally identifying information, PHI and other confidential communications, Kaiser failed to act as a reasonable person would under the circumstances where it was being entrusted with Plaintiffs and Class Members personally identifiable information including PHI.

598. The harm to Plaintiffs and Class Members caused by Kaiser's actions were foreseeable. Kaiser purposefully collected Plaintiff and Class Members' personally identifiable information while also installing Third Party Wiretappers' code on its website and mobile applications and failing to prevent and/or aiding and abetting in that personally identifiable information being intercepted by the Third Party Wiretappers thereby compromising Plaintiffs' and Class Members privacy and the confidentiality of their personally identifiable information.

599. Further, Kaiser breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate safeguards preventing the disclosure of Plaintiffs' and Class Members personally identifiable information to the Third Party Wiretappers.

600. Any social utility in Kaiser's actions is outweighed by the nature of the risk and foreseeability of harm to Plaintiffs and Class Members caused by the disclosure of their personally identifiable information to the Third Party Wiretappers.

601. There is a strong public policy in favor of preventing the harm caused by Kaiser's conduct which compromised Plaintiffs and Class Members personally identifiable information and invaded the Plaintiffs' and Class Members privacy.

602. As a direct and proximate results of Kaiser's failure to exercise reasonable care in its treatment of Plaintiffs and Class Members personally identifiable information, Plaintiffs and Class Members' personally identifiable information was wrongfully disclosed to the Third Party Wiretappers.

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

604. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to comply with the applicable statutes and common law duties governing their conduct, and that Defendants' breach would cause Plaintiffs and Class Members to experience foreseeable harms associated with the unauthorized interception, disclosure, and use of their personal health information by the Third Party Wiretappers.

605. Accordingly, Plaintiffs and Class Members are entitled to: (1) actual damages, in an amount to be proven at trial; (2) punitive damages; (3) equitable relief; and (4) any other relief the Court deems just.

EIGHTH CLAIM FOR RELIEF
Violation of the California Confidentiality of Medical Information Act
Cal. Civ. Code §§ 56.10, *et seq.*
On Behalf of the Kaiser Operating States Class, or alternatively, On Behalf of the California Sub-Class
(Against Kaiser Foundation Health Plan and Kaiser Foundation Hospitals)

606. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

607. Plaintiffs bring this claim individually and on behalf of the Kaiser Operating States Class, or alternatively, on behalf of the California Sub-Class.

608. The Confidentiality of Medical Information Act ("CMIA") provides that a "provider of healthcare, health care service plan, or contractor shall not disclose medical information regarding

a patient of the provider of healthcare or an enrollee or subscriber of a health care service plan without first obtaining an authorization." Cal. Civ. Code § 56.10(a).

609. "Authorization" means "permission granted in accordance with Section 56.11 or 56.21 for the disclosure of medical information." Cal. Civ. Code § 56.05(a).

610. "Patient" means "a natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains." Cal. Civ. Code § 56.05(m).

611. "Medical information" means "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental health application information, mental or physical condition, or treatment." Cal. Civ. Code § 56.05(i).

612. "Individually identifiable" means "that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual," and includes "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 identity of the individual." Cal. Civ. Code § 56.05(i).

613. No language in CMIA limits its application to California residents. Rather, the purpose of the CMIA is to regulate the conduct of California-based medical providers, like Kaiser.

614. California Civil Code Section 56.11 provides criteria for a valid authorization for disclosure of medical information protected by Section 56.10, including that it:

a. "Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type."

b. "Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization."

c. "Is signed and dated by one of the following: (1) The patient . . . (2) The legal representative of the patient . . . (3) The spouse of the patient or the person

financially responsible for the patient . . . (4) The beneficiary or personal representative of a deceased patient."

d. "States the specific uses and limitations on the types of medical information to be disclosed."

e. "States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information."

f. "States the name or functions of the persons or entities authorized to receive the medical information."

g. "States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information."

h. "States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information."

i. "Advises the person signing the authorization of the right to receive a copy of the authorization."[111]

615. Kaiser Permanente's installation of the Third Party Wiretappers' code on its Site, Patient Portal, and Apps disclosed medical information, without authorization, belonging to Plaintiffs, members of the Kaiser Operating States Class, and members of the California Sub-Class, in violation of Cal. Civ. Code § 56.10.

616. Kaiser Permanente knowingly and willfully disclosed medical information without consent to the Third Party Wiretappers, in violation of Cal. Civ. Code § 56.10, for marketing purposes, including to produce targeted advertising for third parties.

617. Pursuant to Cal. Civ. Code § 56.35, Plaintiffs and Kaiser Operating States Class Members—or, alternatively, California Sub-Class Members—have had their medical information disclosed in violation of Section 56.10, sustained economic loss therefrom, and are entitled to: (1)

[111] This reflects the requirements of Section 56.11 as of the filing of the original complaint. The current version of Section 56.11 is effective as of January 1, 2024.

compensatory damages, in an amount to be determined at trial; (2) punitive damages; (3) attorneys' fees; and (4) the costs of litigation.

NINTH CLAIM FOR RELIEF
Statutory Larceny Through False Pretenses
Cal. Penal Code §§ 484, 496
On Behalf of the Kaiser Operating States Class, or alternatively, On Behalf of the California Sub-Class
(Against Kaiser Foundation Health Plan and Kaiser Foundation Hospitals)

618. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

619. Plaintiffs bring this claim individually and on behalf of the Kaiser Operating States Class, or alternatively, on behalf of the California Sub-Class.

620. Cal. Penal Code § 496(a) prohibits the obtaining of property "in any manner constituting theft."

621. "Theft" is prohibited by Cal. Penal Code § 484(a), and a person is guilty of theft, inter alia, where they "fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of . . . personal property."

622. Kaiser acted in a matter constituting theft by false pretenses pursuant to Cal. Penal Code § 484(a), through its installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications, allowing it to, without consent and contrary to its representations in its Terms and Conditions, appropriate or acquire through fraud Plaintiffs' and Kaiser Operating States Class Members', or California Sub-Class Members', private health information.

623. Kaiser knew they obtained Plaintiffs' and Kaiser Operating States Class Members', or California Sub-Class Members', private health information in a manner constituting theft, because it installed the code on its website, Patient Portal, and mobile application, and did so without informing its members that it would be providing Kaiser Plan Members' confidential, medical information to Google, Microsoft Bing, and Twitter for their own and other third parties' use in exchange for "free" use of Google, Microsoft Bing, and Twitter's products.

624. As described above, Kaiser knew or should have known that the data transmitted to these Third Party Wiretappers would be used by these Third Party Wiretappers for their own

independent purposes, based on: information disclosed by the Third Party Wiretappers; the lack of contractual controls to prevent such use or further disclosure; and Kaiser's own understanding of the nature of these technologies and the conduct of the Third Party Wiretappers.

625. Pursuant to Cal. Penal Code § 496(c), Plaintiffs and Kaiser Operating States Class Members—or, alternatively, California Sub-Class Members—have been injured by a violation of § 496(a), and are entitled to: (1) treble damages; (2) attorneys' fees reasonably incurred; and (3) costs of suit.

TENTH CLAIM FOR RELIEF
Violation of the District of Columbia Consumer Protection Procedures Act
D.C. Code §§ 28-3901, *et seq.*
On Behalf of the District of Columbia Sub-Class
(Against Kaiser Foundation Health Plan and Kaiser Foundation Hospitals)

626. Plaintiff Jane Doe II ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

627. Plaintiff brings this claim individually and on behalf of the District of Columbia Sub-Class.

628. Plaintiff and members of the District of Columbia Sub-Class are "persons" within the meaning of D.C. Code § 28-3901(a)(1).

629. Plaintiff and members of the District of Columbia Sub-Class are "consumers" within the meaning of D.C. Code § 28-3901(a)(2)(A).

630. Defendants are "persons" within the meaning of D.C. Code § 28-3901(a)(1).

631. The District of Columbia Consumer Protection Procedures Act provides that "[i]t shall be a violation of this chapter for any person to engage in an unfair or deceptive trade practice, whether or not any consumer is in fact misled, deceived, or damaged thereby, including to:" (1) "represent that goods or services have a source, sponsorship, approval, certification, accessories, characteristics, ingredients, uses, benefits, or quantities that they do not have;" (2) "misrepresent as to a material fact which has a tendency to mislead;" (3) "fail to state a material fact if such failure tends to mislead;" or (4) "use innuendo or ambiguity as to a material fact, which has a tendency to mislead." D.C. Code § 28-3904(a), (e), (f), and (f-1).

632. Kaiser's installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowing it to, without authorization and contrary to its representation in the Site Terms and Conditions, intercept, disclose, and transfer private health information belonging to Plaintiff and members of the District of Columbia Sub-Class to the Third Party Wiretappers is a deceptive trade practices under D.C. Code § 28-3904.

633. Kaiser acted willfully in engaging in trade practices, knowing they are deceptive, by engaging in unauthorized interception, disclosure, and transfer of private health information to Google, Microsoft Bing, and Twitter for their own and other third parties' use in violation of its own Site Terms and Conditions so that Kaiser could obtain "free" use of Google, Microsoft Bing, and Twitter's products.

634. Pursuant to D.C. Code § 28-3905(k), Plaintiff and members of the District of Columbia Sub-Class are consumers seeking relief from the use of a trade practice in violation of the law of the District, and are entitled to: (1) an injunction against the use of Defendants' unlawful trade practices; (2) attorneys' fees reasonably incurred, (3) punitive damages, (4) treble damages, or $1,500 per violation, whichever is greater, (5) additional relief as may be necessary to restore to the Sub-Class members money or property acquired by means of the unlawful trade practice, and (6) any other relief which the Court determines proper.

ELEVENTH CLAIM FOR RELIEF
Violation of the Georgia Computer Systems Protection Act
Ga. Code Ann. § 16-9-93
On Behalf of the Georgia Sub-Class
(Against Kaiser Foundation Health Plan and Kaiser Foundation Hospitals)

635. Plaintiff John Doe II ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

636. Plaintiff brings this claim individually and on behalf of the Georgia Sub-Class.

637. The Georgia Computer Systems Protection Act ("GCSPA") proscribes a number of computer related offenses, including "computer theft" and "computer invasion of privacy." Ga. Code Ann. § 16-9-93(a), (c).

638. The statute provides that "any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of: (1) Taking or appropriating

any property of another, whether or not with the intention of depriving the owner of possession; (2) Obtaining property by any deceitful means or artful practice; or (3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property shall be guilty of computer theft." Ga. Code Ann. § 16-9-93(a).

639. It further provides that "Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy." Ga. Code Ann. § 16-9-93(c).

640. "Without authority" includes "the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network." Ga. Code § Ann. 16-9-92(18).

641. Kaiser's installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowing it to, without authorization and contrary to its representation in the Site Terms and Conditions, intercept, disclose, and transfer private health information belonging to Plaintiff and members of the Georgia Sub-Class is use of a computer network with the intention of taking or appropriating the property of Plaintiff and members of the Georgia Sub-Class, and constitutes computer theft under the GCSPA. Ga. Code Ann. § 16-9-93(a)(1).

642. Kaiser's installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowing it to, without authorization and contrary to its representation in the Site Terms and Conditions, intercept, disclose, and transfer private health information belonging to Plaintiff and members of the Georgia Sub-Class in violation of the Site Terms and Conditions is use of a computer network with the intention of obtaining Plaintiff's and Georgia Sub-Class members' property by deceitful means, and constitutes computer theft under the GCSPA. Ga. Code Ann. § 16-9-93(a)(2).

643. Kaiser's installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowing it to, without authorization and contrary to its representation in the Site Terms and Conditions, intercept, disclose, and transfer private health information

belonging to Plaintiff and members of the Georgia Sub-Class in violation of the Site Terms and Conditions and HIPAA is use of a computer network with the intention of converting Plaintiff's and Georgia Sub-Class members' property to Kaiser's use in violation of an agreement or other known legal obligation, and constitutes computer theft under the GCSPA. Ga. Code Ann. § 16-9-93(a)(3).

644. Kaiser's installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowing it to, without authorization and contrary to its representation in the Site Terms and Conditions, intercept, disclose, and transfer private health information belonging to Plaintiff and members of the Georgia Sub-Class to or personal data with knowledge that such examination is unauthorized, and constitutes computer invasion of privacy under the GCSPA. Ga. Code Ann. § 16-9-93(c).

645. Kaiser knowingly acted without authority because the Third Party Wiretapper's code that Kaiser installed on the Site and Apps commanded Plaintiff and members of the Georgia Sub-Class's browsers to redirect sensitive, personal information, including PHI, to the Third Party Wiretappers without Plaintiff and Georgia Sub-Class members' consent or authorization, thus exceeding any right or permission granted by Plaintiff and Georgia Sub-Class members' who owned the computer or computer networks.

646. Pursuant to Ga. Code Ann. § 16-9-93(g)(1), Plaintiff and Georgia Sub-Class Members have been injured by reason of a violation of provisions of the GCSPA and are entitled to: (1) damages, in an amount to be determined at trial; and (2) the costs of suit.

TWELFTH CLAIM FOR RELIEF
Violation of the Georgia Insurance and Information Privacy Protection Act
Ga. Code Ann. §§ 33-39-1, *et seq*.
On Behalf of the Georgia Sub-Class
(Against Kaiser Foundation Health Plan, Inc.)

647. Plaintiff John Doe II ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

648. Plaintiff brings this claim individually and on behalf of the Georgia Sub-Class.

649. The Georgia Insurance and Information Privacy Protection Act establishes "standards for the collection, use, and disclosure of information gathered in connection with insurance transactions by insurance institutions," and seeks to "[m]aintain a balance between the need for

information by those conducting the business of insurance and the public's need for fairness in insurance information practices, including the need to minimize intrusiveness" and "[l]imit the disclosure of information collected in connection with insurance transactions." Ga. Code Ann. § 33-39-1.

650. The Act provides that "[a]n insurance institution . . . shall not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is . . . with the written authorization of the individual." Ga. Code Ann. § 33-39-14.

651. "Insurance institution" means "any corporation, association, partnership, reciprocal exchange, interinsurer, Lloyd's insurer, fraternal benefit society, or other person engaged in the business of insurance, including health care plans and health maintenance organizations as defined in Chapters 20 and 21 of this title." Ga. Code Ann. § 33-39-3(11).

652. "Insurance transaction" means "any transaction involving insurance primarily for personal, family, or household needs rather than business or professional needs which entails: (A) The individual determination of an individual's eligibility for an insurance coverage, benefit, or payment; or (B) The servicing of an insurance application, policy, contract, or certificate." Ga. Code Ann. § 33-39-3(13).

653. Kaiser Foundation Health Plan, Inc. is an insurance institution under the Act.

654. Given Kaiser Permanente's integrated care model, Plaintiff's and Georgia Sub-Class members' communications and insurance transactions, including making payments for healthcare, through the Kaiser website, Patient Portal, and mobile applications constitute personal or privileged information collected or received in connection with an insurance transaction.

655. Kaiser's installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowing it to, without authorization, disclose Plaintiff's and Georgia Sub-Class members' personal or privileged information to the Third Party Wiretappers is a violation of Ga. Code Ann. § 33-39-14.

656. Kaiser knew that by embedding the Third Party Wiretappers' code, they were disclosing and permitting the Third Party Wiretappers to intercept and collect personally identifying,

and personal and sensitive information relating to Kaiser Plan Members' medical treatment and/or PHI that Kaiser was required to protect and safeguard. As detailed above, the Third Party Wiretappers code intercepts, collects, and transmits significant amounts of healthcare-related communications along with personally identifiable information about Kaiser Plan Members, including IP Addresses, first names, marketing IDs, device identifiers and other information that alone or in combination can be used to identify the individual Kaiser Plan Members.

657. Indeed, as Kaiser admitted to regulators in or around April 12, 2024, the "information collected by these technologies about Kaiser members may be considered Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), pursuant to recent guidance from the Department of Health and Human Services (HHS)." However, as set forth above, Kaiser knew that the Third Party Wiretappers' code was intercepting, transmitting, and collecting PHI and other personally identifying information to the Third Party Wiretappers long before the April 12, 2024 disclosure.

658. Pursuant to Ga. Code Ann. § 33-39-21(b) and (c), Plaintiff and Georgia Sub-Class Members are entitled to: (1) damages sustained as a result of Kaiser Health Plan Inc.'s violation of Section 33-39-14, in an amount to be determined at trial; and (2) reasonable attorneys' fees and other litigation costs reasonably incurred.

THIRTEENTH CLAIM FOR RELIEF
Violation of the Maryland Wiretapping and Electronic Surveillance Act
Md. Code Ann., Cts. & Jud. Proc. §§ 10-401, *et seq*.
On Behalf of the Maryland Sub-Class
(Against Kaiser Foundation Health Plan and Kaiser Foundation Hospitals)

659. Plaintiff Jane Doe III ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

660. Plaintiff brings this claim individually and on behalf of the Maryland Sub-Class.

661. The Maryland Wiretapping and Electronic Surveillance Act ("Maryland Wiretap Act"), Md. Code Ann., Cts. & Jud. Proc. §§ 10-401, *et seq.*, prohibits the interception of any wire, oral, or electronic communications without the consent of all of the parties to the communication.

662. The Act confers a civil cause of action on "any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of this subtitle." Md. Code Ann., Cts. & Jud. Proc. § 10-410(a).

663. The Maryland Wiretap Act provides that it is unlawful for any person to "willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," or "willfully disclose, or endeavor to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subtitle," or "willfully use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subtitle." Md. Code Ann., Cts. & Jud. Proc. § 10-402(a)(1)-(3).

664. In addition, "a person or entity providing an electronic communication service to the public may not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient of the communication or an agent of the addressee or intended recipient." Md. Code Ann., Cts. & Jud. Proc. § 10-402(d)(1).

665. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Md. Code Ann., Cts. & Jud. Proc. § 10-401(10).

666. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system." Md. Code Ann., Cts. & Jud. Proc. § 10-401(5)(i).

667. "Contents" includes "any information concerning the identity of the parties to the communication or the existence, substance, purport, or meaning of that communication." Md. Code Ann., Cts. & Jud. Proc. § 10-401(4).

668. An "electronic communication service" means "any service that provides to users of the service the ability to send or receive wire or electronic communications." Md. Code Ann., Cts. & Jud. Proc. § 10-401(6).

669. Plaintiff's and Maryland Sub-Class Members' communications with Kaiser Permanente through the Site, Portal, and mobile application are electronic communications under the Maryland Wiretap Act.

670. Whenever Plaintiff and Maryland Sub-Class Members communicated with Kaiser Permanente and/or their health care providers on the Site or mobile application, Third Party Wiretappers, through the source code Kaiser Permanente embedded and ran on its website, contemporaneously and intentionally intercepted, and endeavored to intercept Plaintiff's and Maryland Sub-Class Members' electronic communications without authorization or consent.

671. Whenever Plaintiff and Maryland Sub-Class Members communicated with Kaiser Permanente and/or their health care providers on the Site or mobile applications, Kaiser Permanente, through the source code it imbedded and ran on its website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiff's and Maryland Sub-Class Members' electronic communications to the Third Party Wiretappers, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the Maryland Wiretap Act.

672. Whenever Plaintiff and Maryland Sub-Class Members communicated with Kaiser Permanente and/or their health care providers on the Site or mobile applications, Kaiser Permanente, through the source code it embedded and ran on the Site, contemporaneously and intentionally used, and endeavored to use and allow the contents of Plaintiff's and Maryland Sub-Class Members' electronic communications to be disclosed and used for purposes other than providing health care services to Plaintiff and Maryland Sub-Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the Maryland Wiretap Act.

673. Whenever Plaintiff and Maryland Sub-Class Members communicated with Kaiser Permanente and/or their health care providers on the Site or mobile applications, Kaiser Permanente,

through the source code it embedded and ran on the Site and Apps, contemporaneously and intentionally redirected the contents of Plaintiff's and Maryland Sub-Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, namely the Third Party Wiretappers.

674. Whenever Plaintiff and Maryland Sub-Class Members communicated with Kaiser Permanente and/or their health care providers on the Site or mobile applications, Kaiser Permanente, through the source code it embedded and ran on the Site and Apps, contemporaneously and intentionally divulged the contents of Plaintiff's and Maryland Sub-Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, namely the Third Party Wiretappers.

675. The Third Party Wiretappers intentionally intercepted and used the contents of Plaintiff's and Maryland Sub-Class Members' electronic communications for the unauthorized purpose of profiting from Plaintiff and Maryland Sub-Class Members' communications, including by generating advertising revenue.

676. Plaintiff and Maryland Sub-Class Members did not authorize Kaiser to disclose the content of their communications with Kaiser Permanente to the Third Party Wiretappers.

677. Plaintiff and Maryland Sub-Class Members did not authorize the Defendants' interception, redirection, disclosure, and/or use of their sensitive, private health information and communications in their electronic communications with Kaiser Permanente. The Third Party Wiretappers are not party to these communications.

678. The interception of Plaintiff's and Maryland Sub-Class Members' communications was without authorization and consent from Plaintiff and Maryland Sub-Class Members, and thus lacked the prior consent of all parties to the communication. *See* Md. Code Ann., Cts. & Jud. Proc. § 10-402(c)(3).

679. Kaiser knew that by embedding the Third Party Wiretappers' code, they were disclosing and permitting the Third Party Wiretappers to intercept and collect personally identifying, and personal and sensitive information relating to Kaiser Plan Members' medical treatment and/or PHI that Kaiser was required to protect and safeguard. As detailed above, the Third Party Wiretappers

code intercepts, collects, and transmits significant amounts of healthcare-related communications along with personally identifiable information about Kaiser Plan Members, including IP Addresses, first names, marketing IDs, device identifiers and other information that alone or in combination can be used to identify the individual Kaiser Plan Members.

680. Indeed, as Kaiser admitted to regulators in or around April 12, 2024, the "information collected by these technologies about Kaiser members may be considered Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), pursuant to recent guidance from the Department of Health and Human Services (HHS)." However, as set forth above, Kaiser knew that the Third Party Wiretappers' code was intercepting, transmitting, and collecting PHI and other personally identifying information to the Third Party Wiretappers long before the April 12, 2024 disclosure.

681. Defendants' actions were at all relevant times knowing, willful, and intentional.

682. Pursuant to Md. Code Ann., Cts. & Jud. Proc. § 10-410(a), Plaintiff and Maryland Sub-Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the Maryland Wiretap Act and are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class, or (b) liquidated damages of whichever is the greater of $100 per day per violation or $1,000; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

FOURTEENTH CLAIM FOR RELIEF
Violation of the Oregon Unlawful Trade Practices Act, Or. Rev. Stat. §§ 646.605*, et seq*.
On Behalf of the Oregon Sub-Class
(Against Kaiser Foundation Health Plan and Kaiser Foundation Hospitals)

683. Plaintiff Jane Doe V ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

684. Plaintiff brings this claim individually and on behalf of the Oregon Sub-Class.

685. Plaintiff and members of the Oregon Sub-Class are "persons" within the meaning of Or. Rev. Stat. § 646.605(4).

686. Defendants are "persons" within the meaning of Or. Rev. Stat. § 646.605(4).

687. The Oregon Unlawful Trade Practices Act provides that "[a] person engages in an unlawful practice if in the course of the person's business, vocation or occupation the person does any of the following:" (1) [r]epresents that real estate, goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, quantities or qualities that the real estate, goods or services do not have," or (2) "[e]ngages in any other unfair or deceptive conduct in trade or commerce." Or. Rev. Stat. § 646.608(e), (u).

688. Kaiser acted willfully in engaging in trade practices, knowing they are deceptive, by engaging in unauthorized interception, disclosure, and transfer of private health information in violation of its own Site Terms and Conditions.

689. Kaiser knew that by embedding the Third Party Wiretappers' code, they were disclosing and permitting the Third Party Wiretappers to intercept and collect personally identifying, and personal and sensitive information relating to Kaiser Plan Members' medical treatment and/or PHI that Kaiser was required to protect and safeguard. As detailed above, the Third Party Wiretappers code intercepts, collects, and transmits significant amounts of healthcare-related communications along with personally identifiable information about Kaiser Plan Members, including IP Addresses, first names, marketing IDs, device identifiers and other information that alone or in combination can be used to identify the individual Kaiser Plan Members.

690. Indeed, as Kaiser admitted to regulators in or around April 12, 2024, the "information collected by these technologies about Kaiser members may be considered Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), pursuant to recent guidance from the Department of Health and Human Services (HHS)." However, as set forth above, Kaiser knew that the Third Party Wiretappers' code was intercepting, transmitting, and collecting PHI and other personally identifying information to the Third Party Wiretappers long before the April 12, 2024 disclosure.

691. Pursuant to Or. Rev. Stat. § 646.638, Plaintiff and members of the Oregon Sub-Class are entitled to: (1) an injunction against Kaiser Permanente's deceptive trade practices; (2) reasonable attorneys' fees; (3) litigation costs reasonably incurred; (4) actual damages or statutory damages of

$200, whichever is greater; (5) punitive damages; and (6) any other equitable relief the court considers necessary or proper.

FIFTEENTH CLAIM FOR RELIEF
Violation of the Virginia Computer Crimes Act
Va. Code Ann. §§ 18.2-152.1, *et seq.*
On Behalf of the Virginia Sub-Class
(Against Kaiser Foundation Health Plan and Kaiser Foundation Hospitals)

692. Plaintiffs Jane Doe IV and Alexis Sutter ("Plaintiffs" for purposes of this subsection) repeat and incorporates all other paragraphs as if fully set forth herein.

693. Plaintiffs brings this claim individually and on behalf of the Virginia Sub-Class.

694. The Virginia Computer Crimes Act ("VCCA") proscribes a number of computer related offenses, including computer trespass. Va. Code Ann. § 18.2-152.4.

695. The statute provides that "[i]t is unlawful for any person, with malicious intent, or through intentionally deceptive means and without authority, to:" (1) "[u]se a computer or computer network to make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by, or produced by a computer or computer network;" and (2) "[i]nstall or cause to be installed, or collect information through, computer software that records all or a majority of the keystrokes made on the computer of another." Va. Code Ann. § 18.2-152.4(A)(6), (8).

696. "Computer" means "a device that accepts information in digital or similar form and manipulates it for a result based on a sequence of instructions." Va. Code Ann. § 18.2-152.2.

697. "Computer network" means "two or more computers connected by a network." Va. Code Ann. § 18.2-152.2.

698. "Computer data" means "any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or computer network." Va. Code Ann. § 18.2-152.2.

699. Kaiser acted through intentionally deceptive means and without authority because its installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowed it to, without authorization and contrary to its representation in the Site Terms

and Conditions, intercept, disclose, and transfer private health information belonging to Plaintiffs and members of the Virginia Sub-Class is use of a computer network to make or cause to be made an unauthorized copy of computer data in violation of Va. Code Ann. § 18.2-152.4(A)(6).

700. Kaiser did not simply hire Third Parties to do what it could do itself. Indeed, for several Third Party Wiretappers, such as Twitter, Google, and Microsoft Bing, Kaiser did not even have contracts with them covering the code at issue. Moreover, as described above, the Third Parties did more with the code embedded on the Site and Apps than simply perform tasks for Kaiser, these Third Parties used the information transmitted and collected by the code for their own and other third parties' own purposes.

701. As described above, Kaiser knew or should have known that the data transmitted to the Third Party Wiretappers would be used by the Third Party Wiretappers for their own independent purposes, based on: information disclosed by the Third Party Wiretappers; the lack of contractual controls to prevent such use or further disclosure; and Kaiser's own understanding of the nature of these technologies and the conduct of the Third Party Wiretappers.

702. Pursuant to Va. Code Ann. § 18.2-152.12, Plaintiffs and Virginia Sub-Class Members have been injured by reason of computer trespass in violation of the VCCA, and are entitled to: (1) damages, in an amount to be proven at trial; and (2) the costs of suit.

SIXTEENTH CLAIM FOR RELIEF
Violation of the Virginia Insurance Information and Privacy Protection Act
Va. Code Ann. §§ 38.2-600, *et seq.*
On Behalf of the Virginia Sub-Class
(Against Kaiser Foundation Health Plan, Inc.)

703. Plaintiff Jane Doe IV and Alexis Sutter ("Plaintiffs" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

704. Plaintiffs bring this claim individually and on behalf of the Virginia Sub-Class.

705. The Virginia Insurance Information and Privacy Protection Act establishes "standards for the collection, use, and disclosure of information gathered in connection with insurance transactions by insurance institutions, agents or insurance-support organizations," and seeks to "maintain a balance between the need for information by those conducting the business of insurance and the public's need for fairness in insurance information practices, including the need to minimize

intrusiveness" and "limit the disclosure of information collected in connection with insurance transactions." Va. Code Ann. § 38.2-600.

706. The Act provides that "an insurance institution . . . shall not disclose any medical-record information or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is with the written authorization of the individual." Va. Code Ann. § 38.2-613(A).

707. "Insurance institution" means "any corporation, association, partnership, reciprocal exchange, inter-insurer, Lloyd's type of organization, fraternal benefit society, or other person engaged in the business of insurance, including health maintenance organizations, and health, legal, dental, and optometric service plans." Va. Code Ann. § 38.2-602.

708. "Insurance transaction" means "any transaction involving insurance primarily for personal, family, or household needs rather than business or professional needs that entails: 1. The determination of an individual's eligibility for an insurance coverage, benefit or payment; or 2. The servicing of an insurance application, policy, contract, or certificate." Va. Code Ann. § 38.2-602.

709. Kaiser Foundation Health Plan, Inc. is an insurance institution under the Act.

710. Given Kaiser Permanente's integrated care model, Plaintiffs' and Virginia Sub-Class Members' communications and insurance transactions, including making payments for healthcare, through the Kaiser Permanente website, Patient Portal, and mobile applications constitute personal or privileged information collected or received in connection with an insurance transaction.

711. Kaiser Permanente's installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowing it to, without authorization, disclose Plaintiffs' and Virginia Sub-Class members' personal or privileged information to the Third Party Wiretappers is a violation of Va. Code Ann. § 38.2-613(A).

712. Pursuant to Va. Code Ann. § 38.2-617(B), Plaintiffs and Virginia Sub-Class Members are entitled to: (1) damages sustained as a result of Kaiser Health Plan, Inc.'s violation of Section 38.2-613, in an amount to be determined at trial; and (2) reasonable attorneys' fees and other litigation costs reasonably incurred.

SEVENTEENTH CLAIM FOR RELIEF
Violation of the Washington Consumer Protection Act
Wash. Rev. Code §§ 19.86, *et seq*.
On Behalf of the Washington Sub-Class
(Against All Defendants)

713. Plaintiff Jane Doe ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

714. Plaintiff brings this claim individually and on behalf of the Washington Sub-Class.

715. Plaintiff and members of the Washington Sub-Class are "persons" within the meaning of Wash. Rev. Code § 19.86.010(1).

716. Defendants are "persons" within the meaning of Wash. Rev. Code § 19.86.010(1).

717. The Washington Consumer Protection Act ("WCPA") provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." Wash. Rev. Code. § 19.86.020.

718. "Trade" and "commerce" mean "the sale of assets or services, and any commerce directly or indirectly affecting the people of the state of Washington." Wash. Rev. Code § 19.86.010(2).

719. Kaiser's installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowing it to, without authorization and contrary to its representation in the Site Terms and Conditions, intercept, disclose, and transfer private health information belonging to Plaintiff and members of the Washington Sub-Class to the Third Party Wiretappers is an unfair or deceptive act or practice under Wash. Rev. Code § 19.86.020.

720. Kaiser knew that by embedding the Third Party Wiretappers' code, they were disclosing and permitting the Third Party Wiretappers to intercept and collect personally identifying, and personal and sensitive information relating to Kaiser Plan Members' medical treatment and/or PHI that Kaiser was required to protect and safeguard. As detailed above, the Third Party Wiretappers code intercepts, collects, and transmits significant amounts of healthcare-related communications along with personally identifiable information about Kaiser Plan Members, including IP Addresses, first names, marketing IDs, device identifiers and other information that alone or in combination can be used to identify the individual Kaiser Plan Members.

721. Indeed, as Kaiser admitted to regulators in or around April 12, 2024, the "information collected by these technologies about Kaiser members may be considered Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), pursuant to recent guidance from the Department of Health and Human Services (HHS)." However, as set forth above, Kaiser knew that the Third Party Wiretappers' code was intercepting, transmitting, and collecting PHI and other personally identifying information to the Third Party Wiretappers long before the April 12, 2024 disclosure.

722. Kaiser Permanente acted willfully in engaging in trade practices, knowing they are deceptive, by engaging in unauthorized interception, disclosure, and transfer of private health information in violation of its own Site Terms and Conditions.

723. Pursuant to Wash. Rev. Code § 19.86.090, Plaintiff and members of the Washington Sub-Class are persons who are injured in their business or property by a violation of § 19.86.020, and are entitled to: (1) enjoin further violations by Kaiser Permanente; (2) reasonable attorneys' fees; (3) litigation costs reasonably incurred; (4) actual damages; and (5) treble damages.

EIGHTEENTH CLAIM FOR RELIEF
Violation of the Washington Privacy Act
Wash. Rev. Code §§ 9.73, *et seq*.
On Behalf of the Washington Sub-Class
(Against All Defendants)

724. Plaintiff Jane Doe ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

725. Plaintiff brings this claim individually and on behalf of the Washington Sub-Class.

726. Under Sections 9.73.030(1) and 9.73.030(1)(a) of the Washington Privacy Act ("WPA"), it is unlawful "for any individual, partnership, corporation, association, or the state of Washington, its agencies, and political subdivisions to intercept, or record any . . . [p]rivate communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication."

727. Under Section 9.73.030(1)(a) of the WPA, a defendant must show it had the consent of all parties to a communication.

728. Kaiser and the Third Party Wiretappers are each a "person" for the purposes of the WPA.

729. Kaiser treats and insures patients in Washington and provides access to its website, Patient Portal, and mobile applications to patients in Washington, where Kaiser and the Third Party Wiretappers intercepted Plaintiff and Washington Sub-Class Members' communications.

730. The Third Party Wiretappers' code, Quantum Metric's recording code, Plaintiff 's and Sub-Class Members' browsers and Plaintiff and Washington Sub-Class Members' computing and mobile devices are all "device[s] electronic or otherwise designed to record and/or transmit said communication" used to engaged in the prohibited conduct at issue here. Wash. Rev. Code § 9.73.030(1)(a).

731. Kaiser installed the Third Party Wiretappers' code to automatically and secretly spy on, and intercept Plaintiffs and Washington Sub-Class Members' communications with Kaiser Permanente through the Kaiser Permanente website in real time.

732. At all relevant times, Kaiser's disclosure of Plaintiff and Washington Sub-Class Members' internet communications to Third Party Wiretappers was without Plaintiff and Washington Sub-Class Members' authorization or consent.

733. By installing the Third Party Wiretappers' code on its website and mobile applications, Kaiser intentionally caused Plaintiff and Washington Sub-Class Members' communications to be intercepted, recorded, stored, and transmitted to the Third Party Wiretappers.

734. At all relevant times, the Third Party Wiretappers intentionally tapped or made unauthorized connections with, the lines of internet communication between Plaintiff and Washington Sub-Class Members and Kaiser's Site and mobile applications without the consent of all parties to the communication.

735. The Third Party Wiretappers willfully read or attempt to read or learn the contents or meaning of Plaintiff and Washington Sub-Class Members' communications to Kaiser Permanente's Site and mobile applications 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 Plaintiff and Sub-Class Members' communications with Kaiser Permanente's Site and mobile applications in real time.

736. By embedding the Third Party Wiretappers' technology on its Site and Apps, Kaiser intercepted and/or aided, agreed with, employed, and conspired with Third Party Wiretappers to carry out the wrongful conduct alleged herein in violation of Wash. Rev. Code §§ 9.73.030 and 9.73.060.

737. Kaiser did not simply hire Third Parties to do what it could do itself. Indeed, for several Third Party Wiretappers, such as Twitter, Google, and Microsoft Bing, Kaiser did not even have contracts with them covering the code at issue. Moreover, as described above, the third parties did more with the code embedded on the Site and Apps than simply perform tasks for Kaiser, these third parties used the information transmitted and collected by the code for their own and other third parties' own purposes.

738. As described above, Kaiser knew or should have known that the data transmitted to the Third Party Wiretappers would be used by the Third Party Wiretappers for their own independent purposes, based on: information disclosed by the Third Party Wiretappers; the lack of contractual controls to prevent such use or further disclosure; and Kaiser's own understanding of the nature of these technologies and the conduct of the Third Party Wiretappers.

739. Plaintiff and the Sub-Class Members seek statutory damages in accordance with Wash. Rev. Code § 9.73.060, which provides for damages sustained by Plaintiff and the Sub-Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

NINETEENTH CLAIM FOR RELIEF
Violation of the Washington Health Care Information Act
Wash. Rev. Code §§ 70.02.005, *et seq*.
On Behalf of the Washington Sub-Class
(Against All Defendants)

740. Plaintiff Jane Doe ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

741. Plaintiff brings this claim individually and on behalf of the Washington Sub-Class.

742. The Washington Health Care Information Act, Wash. Rev. Code §§ 70.2.005, *et seq*., states that "a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care

information about a patient to any other person without the patient's written authorization." *Id.* § 70.02.020(1).

743. The Act defines "health care information" to mean "any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care . . . ." Wash. Rev. Code § 70.02.010(17).

744. Kaiser Permanente is a health care provider as defined by Wash. Rev. Code § 70.010(19).

745. By deploying code on its website and mobile applications to capture and transmit its patients' personally identifiable and health information to third parties, Kaiser Permanente discloses Plaintiff and Washington Sub-Class Members' health care information without their written authorization.

746. Kaiser knew that by embedding the Third Party Wiretappers' code, they were disclosing and permitting the Third Party Wiretappers to intercept and collect personally identifying, and personal and sensitive information relating to Kaiser Plan Members' medical treatment and/or PHI that Kaiser was required to protect and safeguard. As detailed above, the Third Party Wiretappers code intercepts, collects, and transmits significant amounts of healthcare-related communications along with personally identifiable information about Kaiser Plan Members, including IP Addresses, first names, marketing IDs, device identifiers and other information that alone or in combination can be used to identify the individual Kaiser Plan Members.

747. Indeed, as Kaiser admitted to regulators in or around April 12, 2024, the "information collected by these technologies about Kaiser members may be considered Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), pursuant to recent guidance from the Department of Health and Human Services (HHS)." However, as set forth above, Kaiser knew that the Third Party Wiretappers' code was intercepting, transmitting, and collecting PHI and other personally identifying information to the Third Party Wiretappers long before the April 12, 2024 disclosure.

748. As a direct and proximate cause of Kaiser Permanente's actions, Plaintiff and Washington Sub-Class Members were damaged in that:

749. Sensitive, confidential, and/or protected information that Plaintiff and Washington Sub-Class Members intended to remain private is no more;

750. Kaiser Permanente took something of value from Plaintiff and Washington Sub-Class Members and derived benefit therefrom without Plaintiff and Washington Sub-Class Members' knowledge or informed consent and without sharing the benefit of such value;

751. Plaintiff and Washington Sub-Class Members did not get the full value of the medical services for which they paid, which included Kaiser Permanente's duty to maintain confidentiality of patient data and communications; and

752. Kaiser Permanente's actions diminished the value of Plaintiff and Washington Sub-Class Members' personally identifiable information, patient data and communications.

753. Plaintiff and Washington Sub-Class Members seek an order requiring Kaiser Permanente to comply with the Act, actual damages, and attorney's fees and costs.

TWENTIETH CLAIM FOR RELIEF
Violation of the District of Columbia Consumer Security Breach Notification Act
D.C. Code §§ 28-3851, *et seq.*, and Consumer Protection Procedures Act,
D.C. Code §§ 28-3901, *et seq.*
On Behalf of Plaintiff Jane Doe II and the District of Columbia Sub-Class
(Against Kaiser Foundation Health Plan and Kaiser Foundation Hospitals)

754. Plaintiff Jane Doe II ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

755. Plaintiff brings this claim individually and on behalf of the District of Columbia Sub-Class.

756. Under D.C. Code § 28-3852(a), Kaiser was required to accurately notify Plaintiff and District of Columbia Sub-Class Members if it discovers a breach of the security of the system (unauthorized acquisition of computerized or other electronic data or any equipment or device storing such data that compromises the security, confidentiality, or integrity of personal information) in the most expedient time possible and without unreasonable delay.

757. Kaiser is an entity that owns or licenses computerized data or other electronic data that includes Personal Information as defined by D.C. Code § 28-3851(3)(A).

758. Plaintiff and District of Columbia Sub-Class Members' Personal Information (e.g., their names, health insurance information, and medical records) includes Personal Information as covered under D.C. Code § 28-3851(3) (including "[a]n individual's first name, first initial and last name, or any other personal identifier" in combination with "any information about a consumer's dental, medical, or mental health treatment or diagnosis by a health-care professional[,]" or "[h]ealth insurance information, including a policy number, subscriber information number, or any unique identifier used by a health insurer to identify the person that permits access to an individual's health and billing information".

759. Because Kaiser was aware of a breach of its security system, Kaiser had an obligation to disclose the data breach in a timely and accurate fashion as mandated by D.C. Code § 28-3852(a).

760. Kaiser unreasonably delayed in informing Plaintiff and other Kaiser Plan Members about the data breach after Kaiser knew or should have known that the data breach had occurred.

761. Kaiser was aware of the data breach by at least October 25, 2023, but unreasonably delayed in providing notification to state and federal regulators until April 12, 2024 and unreasonably delayed in providing notification to Plaintiffs and other Kaiser Plan Members until May 8, 2024.

762. By failing to disclose the Data Breach in a timely and accurate manner Kaiser violated D.C. Code § 28-3852(a).

763. Plaintiffs and other Kaiser Plan Members were damaged by Kaiser's failure to safeguard their PII and PHI and failure to comply with the data breach notification statute.

764. As a direct and proximate cause of Kaiser's violation of D.C. Code § 28-3852(a), Plaintiff and District of Columbia Sub-Class Members were damaged in the following ways, *inter alia*:

- Sensitive, confidential, and/or protected information that Plaintiff and District of Columbia Sub-Class Members intended to remain private is no more;
- Kaiser took something of value from Plaintiff and District of Columbia Sub-Class Members and derived benefit therefrom without Plaintiff and District of Columbia Sub-Class Members' knowledge or informed consent and without sharing the benefit of such value;

- Plaintiff and District of Columbia Sub-Class Members did not get the full value of the medical services for which they paid, which included Kaiser's duty to maintain confidentiality of patient data and communications; and
- Kaiser's actions diminished the value of Plaintiff and District of Columbia Sub-Class Members' personally identifiable information, patient data and communications.

765. Pursuant to D.C. Code § 28-3853(b), Kaiser's violation of D.C. Code § 28-3852(a) is an unfair or deceptive trade practice within the meaning of the District of Columbia Consumer Protection Procedures Act, D.C. Code § 28-3904(kk), and subject to the enforcement and penalty provisions contained within the District of Columbia Consumer Protection Procedures Act.

766. Plaintiff and District of Columbia Sub-Class Members seek relief under D.C. Code § 28-3905(k), including (1) an injunction against the use of Defendants' unlawful trade practices; (2) attorneys' fees reasonably incurred, (3) punitive damages, (4) treble damages, or $1,500 per violation, whichever is greater, (5) additional relief as may be necessary to restore to Plaintiff and the Sub-Class Members money or property acquired by means of the unlawful trade practice, and (6) any other relief which the Court determines proper.

TWENTY-FIRST CLAIM FOR RELIEF
Violation of the Maryland Personal Information Protection Act
Md. Code Ann. Com. Law §§ 14-3501, *et seq*., and Consumer Protection Act,
Md. Code Ann. Com. Law §§ 13-101, *et seq.*
On Behalf of Plaintiff Jane Doe III and the Maryland Sub-Class
(Against Kaiser Foundation Health Plan and Kaiser Foundation Hospitals)

767. Plaintiff Jane Doe III ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

768. Plaintiff brings this claim individually and on behalf of the Maryland Sub-Class.

769. Under Md. Code Ann. Com. Law § 14-3504(b), Kaiser was required to accurately notify Plaintiff and Maryland Sub-Class Members if it discovers a breach of the security of the system (unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business) as soon as reasonably practicable, but not later than 45 days after the business discovers or is notified of the breach of security of a system.

770. Kaiser is a business that owns, licenses, or maintains computerized data that includes Personal Information as defined by Md. Code Ann. Com. Law § 14-3501(b)(1).

771. Plaintiff and Maryland Sub-Class Members' Personal Information (e.g., their names, health insurance information, and medical records) includes Personal Information as covered under Md. Code Ann. Com. Law § 14-3501(e)(1) (including e.g., "[a]n individual's first name or first initial and last name in combination with … [h]ealth information, including information about an individual's mental health; [or a] health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information").

772. Because Kaiser was aware of a breach of its security system, Kaiser had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Md. Code Ann. Com. Law § 14-3504(b).

773. Kaiser unreasonably delayed in informing Plaintiff and other Kaiser Plan Members about the data breach after Kaiser knew or should have known that the data breach had occurred.

774. Kaiser was aware of the data breach by at least October 25, 2023, but unreasonably delayed in providing notification to state and federal regulators until April 12, 2024 and unreasonably delayed in providing notification to Plaintiffs and other Kaiser Plan Members until May 8, 2024.

775. By failing to disclose the Data Breach in a timely and accurate manner Kaiser violated Md. Code Ann. Com. Law § 14-3504(b).

776. Plaintiffs and other Kaiser Plan Members were damaged by Kaiser's failure to safeguard their PII and PHI and failure to comply with the data breach notification statute.

777. As a direct and proximate cause of Kaiser's violation of Md. Code Ann. Com. Law § 14-3504(b), Plaintiff and Maryland Sub-Class Members were damaged in the following ways, *inter alia*:

- Sensitive, confidential, and/or protected information that Plaintiff and Maryland Sub-Class Members intended to remain private is no more;

- Kaiser took something of value from Plaintiff and Sub-Class Members and derived benefit therefrom without Plaintiff and Maryland Sub-Class Members' knowledge or informed consent and without sharing the benefit of such value;
- Plaintiff and Maryland Sub-Class Members did not get the full value of the medical services for which they paid, which included Kaiser's duty to maintain confidentiality of patient data and communications; and
- Kaiser's actions diminished the value of Plaintiff and Maryland Sub-Class Members' personally identifiable information, patient data and communications.

778. Pursuant to Md. Code Ann. Com. Law § 14-3508(1), Kaiser's violation of Md. Code Ann. Com. Law § 14-3504(b) is an unfair or deceptive trade practice within the meaning of the Maryland Consumer Protection Act, Md. Code Ann. Com. Law §§ 13-101, *et seq.*, and subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

779. Plaintiff and Maryland Sub-Class Members seek relief under Md. Code Ann. Com. Law § 13-408, including actual damages and reasonable attorney's fees.

TWENTY-FIRST CLAIM FOR RELIEF
[INTENTIONALLY OMITTED]

TWENTY-SECOND CLAIM FOR RELIEF
Violation of the Washington Data Breach Act ("DBA")
Wash. Rev. Code §§ 19.255.005, *et seq*.
On Behalf of the Washington Sub-Class
(Against All Defendants)

780. Plaintiff Jane Doe ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

781. Plaintiff Jane Doe ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

782. Plaintiff brings this claim individually and on behalf of the Washington Sub-Class.

783. Under Wash. Rev. Code Ann. § 19.255.010(8), Kaiser was required to accurately notify Plaintiff and Washington Sub-Class members following discovery or notification of the breach of its data security system (if personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured) "in the most

expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered."

784. Kaiser is a business that owns or licenses computerized data that includes personal information as defined by Wash. Rev. Code Ann. § 19.255.005(2)(a).

785. Plaintiff's and Washington Sub-Class Members' private information (e.g., their names, health insurance information, and medical records) includes personal information as covered under Wash. Rev. Code Ann. § 19.255.005(2)(a) (including e.g., "an individual's first name or first initial and last name in combination with … [h]ealth insurance policy number or health insurance identification number; [or a]ny information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer").

786. Because Kaiser discovered a breach of its security system (in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured), Kaiser had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code Ann. § 19.255.010(1). However, Kaiser breached that obligation by unreasonably delaying, for more than thirty calendar days, notification to Plaintiff and Washington Sub-Class Members.

787. Kaiser unreasonably delayed in informing Plaintiff and other Kaiser Plan Members about the data breach after Kaiser knew or should have known that the data breach had occurred.

788. Kaiser was aware of the data breach by at least October 25, 2023, but unreasonably delayed in providing notification to state and federal regulators until April 12, 2024 and unreasonably delayed in providing notification to Plaintiffs and other Kaiser Plan Members until May 8, 2024.

789. Plaintiffs and other Kaiser Plan Members were damaged by Kaiser's failure to safeguard their PII and PHI and failure to comply with the data breach notification statute.

790. As a direct and proximate cause of Kaiser's violation of Wash. Rev. Code Ann. § 19.255.005(1), Plaintiff and Washington Sub-Class Members were damaged in the following ways, *inter alia*:

- Sensitive, confidential, and/or protected information that Plaintiff and Washington Sub-Class Members intended to remain private is no more;

- Kaiser took something of value from Plaintiff and Sub-Class Members and derived benefit therefrom without Plaintiff and Washington Sub-Class Members' knowledge or informed consent and without sharing the benefit of such value;
- Plaintiff and Washington Sub-Class Members did not get the full value of the medical services for which they paid, which included Kaiser's duty to maintain confidentiality of patient data and communications; and
- Kaiser's actions diminished the value of Plaintiff and Washington Sub-Class Members' personally identifiable information, patient data and communications.

791. Plaintiff and Washington Sub-Class Members seek actual damages under Wash. Rev. Code Ann. § 19.255.040(3)(a).

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Classes, respectfully requests that the Court enter an order:

A. Certifying this case as a class action on behalf of the Classes defined above, appointing Plaintiffs as the representatives of the Classes, and appointing Plaintiffs' counsel as the Class Counsel for the Classes;

B. Declaring that Defendants' conduct, as set forth above, violates the laws cited herein;

C. Enjoining Defendants' unlawful conduct;

D. Awarding damages, including nominal, actual, statutory, and punitive damages where applicable, to Plaintiffs and the Classes in an amount to be determined at trial;

E. Awarding Plaintiffs and the Classes their reasonable litigation expenses, costs and attorneys' fees;

F. Awarding Plaintiffs and the Classes pre- and post-judgment interest, to the extent allowable;

G. Awarding such other further injunctive and declaratory relief as is necessary to protect the interests of Plaintiffs and the Classes; and

H. Awarding such other and further relief as the Court deems reasonable and just.

IX. DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiffs demand a jury trial as to all issues triable by a jury.

DATED: December 6, 2024

Respectfully submitted,

KESSLER TOPAZ
MELTZER & CHECK, LLP

/s/ Melissa L. Yeates
Joseph H. Meltzer (appearance *pro hac vice*)
jmeltzer@ktmc.com
Melissa L. Yeates (appearance *pro hac vice*)
myeates@ktmc.com
Tyler S. Graden (appearance *pro hac vice*)
tgraden@ktmc.com
Jordan E. Jacobson (Bar No. 302543)
jjacobson@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056

-and-

Jennifer L. Joost (Bar No. 296164)
jjoost@ktmc.com
KESSLER TOPAZ
MELTZER & CHECK, LLP
One Sansome Street, Suite 1850
San Francisco, CA 94104
Telephone: (415) 400-3000
Facsimile: (415) 400-3001

-and-

James E. Cecchi (appearance *pro hac vice*)
jcecchi@carellabyrne.com
Michael A. Innes (*pro hac vice* forthcoming)
minnes@carellabyrne.com
Kevin G. Cooper (appearance *pro hac vice*)
kcooper@carellabyrne.com
CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973)-994-1700
Facsimile: (973)-994-1744

-and-

Zachary Jacobs (appearance *pro hac vice*)
zjacobs@carellabyrne.com
CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.
222 S Riverside Plaza
Chicago, Illinois 06606

Interim Class Counsel

Robert Mackey, Cal Bar No. 125961
LAW OFFICES OF ROBERT MACKEY
bobmackeyesq@aol.com
16320 Murphy Road
Sonora, CA 95370
Telephone: (412) 370-9110

Jason S. Rathod
jrathod@classlawdc.com
MIGLIACCIO & RATHOD LLP
412 H Street NE, no. 302,
Washington, DC, 20002
Telephone: (202) 470-3520

Additional Counsel for Plaintiff Alexis Sutter