

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**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
jmeltzer@ktmc.com
Melissa L. Yeates
myeates@ktmc.com
Tyler S. Graden
tgraden@ktmc.com
Jordan E. Jacobson
jjacobson@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056

Counsel for Plaintiff and the proposed Classes

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION**

JOHN DOE, Individually and on behalf of all
others similarly situated,

Plaintiff,

v.

KAISER FOUNDATION HEALTH PLAN,
INC., KAISER FOUNDATION HOSPITALS,
and THE PERMANENTE MEDICAL GROUP,
INC.

Defendant.

Case No. 4:23-cv-02207

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

1

2 I. NATURE OF THE ACTION 1

3 II. THE PARTIES 4

4 A. Plaintiff 4

5 B. Defendants 5

6 III. JURISDICTION AND VENUE 6

7 IV. FACTUAL ALLEGATIONS 6

8 A. Kaiser Permanente Communicates with Kaiser Plan Members Through

9 the Kaiser Permanente Website 6

10 B. Multiple Third Party Wiretappers Intercept Kaiser Plan Members’

11 Information Shared with, and Communications with, Kaiser Permanente

12 and Its Providers 14

13 1. Kaiser Permanente Allows Quantum Metric to Intercept Kaiser Plan

14 Members’ Information and Communications 14

15 2. Kaiser Permanente Allows Adobe to Intercept Kaiser Plan Members’

16 Information and Communications 19

17 3. Kaiser Permanente Allows Twitter, Bing, and Google to Intercept

18 Patients’ Communications 27

19 C. Plaintiff and Class Members Did Not Consent to Kaiser Permanente

20 Disclosure of Their Information and Communications to Third Parties 35

21 D. Plaintiff’s and Class Members’ Health Information Has Actual, Measurable,

22 Monetary Value 36

23 E. Kaiser Permanente’s Conduct Violates State and Federal Privacy Laws 37

24 V. TOLLING 41

25 VI. CLASS ACTION ALLEGATIONS 42

26 VII. CLAIMS FOR RELIEF 44

27 VIII. PRAYER FOR RELIEF 64

28

1 Plaintiff¹ brings this proposed class action against Kaiser Foundation Health Plan, Inc., Kaiser
2 Foundation Hospitals, and The Permanente Medical Group, Inc. (collectively “Kaiser Permanente”
3 or “Defendants”), individually and on behalf of all others similarly situated, upon personal knowledge
4 as to Plaintiff’s own conduct, and on information and belief as to all other matters based on
5 investigation by counsel.²

6 **I. NATURE OF THE ACTION**

7 1. As any reasonable patient would expect, Plaintiff trusted that his medical providers
8 would treat the information that he shared with them as private and confidential.

9 2. This expectation extends to Plaintiff’s use of Kaiser Permanente’s websites, on which
10 he and other patients would schedule appointments, access medical test results, learn about treatment
11 options, exchange messages and healthcare information with providers, participate in online health
12 assessments, pay bills, and research specialists, among other sensitive activities.

13 3. Notwithstanding, Plaintiff and other patients’ reasonable expectation that their
14 interactions and communications through Kaiser Permanente’s website would not be shared with
15 third parties, Kaiser Permanente discloses the contents of patients’ confidential information and
16 communications with a number of third parties, completely unbeknownst to Plaintiff and its other
17 patients, while those communications are in transit between Plaintiff and Class Members on the one
18 hand and Kaiser Permanente on the other.

19 4. Specifically, unbeknownst to Plaintiff and its other patients, Kaiser Permanente has
20 installed code from multiple third parties throughout the Kaiser Permanente website that allows third
21 party companies such as Quantum Metric, Twitter, Adobe, Bing, and Google (collectively, “Third

22 ¹ Plaintiff seeks to proceed anonymously, as other plaintiffs have in other litigation claiming privacy
23 violations involving health care providers. *See, e.g.*, Class Action Complaint & Demand for Jury
24 Trial, *Doe v. Meta Platforms Inc., Inc.*, No. 22-cv-3580 (N.D. Cal. June 17, 2022), ECF No. 1; Class
25 Action Complaint & Demand for Jury Trial, *Doe v. Meta Platforms Inc.*, No. 22-cv-04680 (N.D. Cal.
26 Aug. 15, 2022), ECF No. 1; Complaint, *Doe v. Meta Platforms Inc.*, No. 22-cv-4963 (N.D. Cal. Aug.
27 30, 2022), ECF No. 1; Class Action Complaint & Demand for Jury Trial, *Doe v. Meta Platforms Inc.*,
28 No. 22-cv-6665 (N.D. Cal. Oct. 28, 2022), ECF No. 1; Complaint, *Doe v. Meta Platforms Inc.*, No.
22-cv-4293 (N.D. Cal. July 25, 2022), ECF No. 1. Plaintiff will seek Defendants’ consent to proceed
anonymously.

² Counsel’s investigation includes an analysis of publicly available information. Plaintiff believes that
a reasonable opportunity for discovery will provide further support for the claims alleged herein.

1 Party Wiretappers”) to intercept the content of Plaintiff and Class Members’ patient status, identifying
2 information, medical topics researched, choices made, information shared and communications with
3 their medical providers, including personally identifiable medical information and other confidential
4 information and communications, when that information is in transit.

5 5. The third party code that Kaiser Permanente has installed on its website transmits and
6 redirects the content of Plaintiff and other Class Members’ communications to these Third Party
7 Wiretappers from the very moment that a user first loads Kaiser Permanente’s website and continues
8 as the user navigates through the website researching and sharing sensitive information.

9 6. Once the website loads, the Third Party Wiretappers continue to intercept the content
10 of patients’ communications with Kaiser Permanente in real time as the patient navigates the website
11 to access specific medical information, clicks buttons that divulge sensitive and protected patient
12 status, and personal and health information, and enters information into various fields on Kaiser
13 Permanente’s website, such as: (1) signing-up for a patient Portal; (2) signing-in or signing-out of a
14 patient portal; (3) taking actions inside a patient Portal; (4) making, scheduling, or participating in
15 appointments; (5) exchanging communications relating to doctors, treatments, payment information,
16 health insurance information, prescription drugs, prescriptions, side effects, conditions, diagnoses,
17 prognoses, or symptoms of health conditions; and (6) providing other information that qualifies as
18 “personal health information” and/or identifying information under federal and state laws.

19 7. Kaiser Permanente knew that by embedding the Third Party Wiretappers’ code, they
20 were disclosing and permitting these Third Party Wiretappers to intercept and collect information
21 shared by its website users, including the content of Plaintiff and Class Members’ communications,
22 which include identifying information, personal and sensitive information relating to medical
23 treatment, and/or information that Kaiser Permanente was required to protect under the Health
24 Insurance Portability and Accountability Act of 1996 (“HIPAA”), 42 U.S.C. § 1320d-6.

25 8. In fact, in December 2022, the United States Department of Health and Human
26 Services (“HHS”) issued a bulletin “to highlight the obligations” of health care providers under the
27 HIPAA Privacy Rule “when using online tracking technologies” such as those used by Kaiser
28

1 Permanente which “collect and analyze information about how internet users are interacting with a
2 regulated entity’s website or mobile application.”³

3 9. In the bulletin, HHS confirmed that HIPAA applies to health care providers’ use of
4 tracking technologies like those developed by the Third Party Wiretappers and used by Kaiser
5 Permanente. Among other things, HHS explained that health care providers violate HIPAA when
6 they use tracking technologies that disclose an individual’s identifying information even if no
7 treatment information is included and even if the individual does not have a relationship with the
8 health care provider:

9 How do the HIPAA Rules apply to regulated entities’ use of tracking technologies?

10 Regulated entities disclose a variety of information to tracking technology vendors
11 through tracking technologies placed on a regulated entity’s website or mobile app,
12 including individually identifiable health information (IIHI) that the individual
13 provides when they use regulated entities’ websites or mobile apps. This
14 information might include an individual’s medical record number, home or email
15 address, or dates of appointments, as well as an individual’s IP address or
16 geographic location, medical device IDs, or any unique identifying code. **All such
17 IIHI collected on a regulated entity’s website or mobile app generally is PHI,
18 even if the individual does not have an existing relationship with the regulated
19 entity and even if the IIHI, such as IP address or geographic location, does not
20 include specific treatment or billing information like dates and types of health
21 care services.** This is because, when a regulated entity collects the individual’s IIHI
22 through its website or mobile app, the information connects the individual to the
23 regulated entity (*i.e.*, it is indicative that the individual has received or will receive
24 health care services or benefits from the covered entity), and thus relates to the
25 individual’s past, present, or future health or health care or payment for care.

10. HHS further clarified that HIPAA applies to health care providers’ webpages with
19 tracking technologies even on webpages that do not require patients to login:

20 Tracking on unauthenticated webpages

21 . . . [T]racking technologies on unauthenticated webpages may have access to PHI,
22 in which case the HIPAA Rules apply to the regulated entities’ use of tracking
23 technologies and disclosures to the tracking technology vendors. Examples of
24 unauthenticated webpages where the HIPAA Rules apply include: The login page
25 of a regulated entity’s patient portal (which may be the website’s homepage or a
separate, dedicated login page), or a user registration webpage where an individual
creates a login for the patient portal . . . [and pages] that address[] specific

26 ³ Press Release, *HHS Office of Civil Rights Issue Bulletin on Requirements under HIPAA for Online*
27 *Tracking Technologies to Protect the Privacy and Security of Health Information*, HHS (Dec. 1,
28 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), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

1 symptoms or health conditions, such as pregnancy or miscarriage, or that permits
2 individuals to search for doctors or schedule appointments without entering
3 credentials may have access to PHI in certain circumstances. **For example,**
4 **tracking technologies could collect an individual's email address and/or IP**
5 **address when the individual visits a regulated entity's webpage to search for**
6 **available appointments with a health care provider.** In this example, the
7 regulated entity is disclosing PHI to the tracking technology vendor, and thus the
8 HIPAA Rules apply.

9 11. This HHS bulletin did not create any new obligations, but instead highlights
10 obligations that have been in place for decades, with which Kaiser Permanente should have been
11 complying.

12 12. Kaiser Permanente's disclosure of patients' patient status, identifying information and
13 personal and sensitive health information to the Third Party Wiretappers, including without adequate
14 disclosure of its conduct to Plaintiff and Class Members, constitutes an egregious invasion of Plaintiff
15 and Class Members' privacy and violates the Electronic Communications Privacy Act, 18 U.S.C. §§
16 2510, *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; Cal. Const. art.
17 I, § 1, and HIPAA, and constitutes intrusion upon seclusion and breach of Kaiser Permanente's
18 express and implied promises and duties to its patients, including Plaintiff and members of the
19 Classes.

16 II. THE PARTIES

17 A. Plaintiff

18 13. Plaintiff John Doe is a citizen of California, and resides in Camarillo, California.

19 14. Plaintiff is a Kaiser Foundation Health Plan member and has received medical
20 treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group since 2010.

21 15. Plaintiff regularly uses Kaiser Permanente's website and Patient Portal to access
22 medical information and communicate with his health care providers, including making
23 appointments, researching providers and medical conditions, checking medical results, and reviewing
24 his medical history.

25 16. Without Plaintiff's knowledge or consent, Kaiser Permanente allowed the Third Party
26 Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or meaning of the
27 contents of Plaintiff's patient status, identifying information, personal and sensitive health
28

1 information, and confidential communications with his health care providers through Kaiser
2 Permanente’s website while that information and those messages, reports, and/or communications
3 were in transit.

4 **B. Defendants**

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

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

12 19. Kaiser Foundation Health Plan, Inc. is financially responsible for the payment of
13 medical services provided to its enrollees (“Kaiser Plan Members”) or has accepted such financial
14 responsibility under contract with one or more of the Kaiser Permanente entities. Kaiser Foundation
15 Health Plan, Inc. is the largest health care service plan in the United States, with over 11.8 million
16 members in eight states (California, Colorado, Georgia, Hawaii, Maryland, Oregon, Virginia, and
17 Washington) and the District of Columbia.

18 20. Kaiser Foundation Hospitals is a non-profit, public-benefit corporation headquartered
19 in Oakland, California. Kaiser Foundation Hospitals operates nearly 40 acute care hospitals and 680
20 medical offices in eight states (California, Colorado, Georgia, Hawaii, Maryland, Oregon, Virginia,
21 and Washington) and Washington D.C., with its largest presence being in California, where the
22 majority of its hospitals are located. Kaiser Foundation Hospitals employs more than 21,000
23 physicians, representing all medical fields.

24 21. The Permanente Medical Group, Inc. is headquartered in Oakland, California and is
25 comprised of physician-owned, for-profit, partnerships, and professional corporations.

26 22. Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and The
27 Permanente Medical Group, Inc. operate under the name “Kaiser Permanente,” which is not a legal
28

1 entity but a registered trademark or trade name that Kaiser Foundation Health Plan, Inc. owns and
2 Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and The Permanente Medical
3 Group, Inc. use, acting in concert.

4 **III. JURISDICTION AND VENUE**

5 23. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C.
6 § 1331 because this suit is brought under the laws of the United States, specifically the Electronic
7 Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.* This Court also has subject matter
8 jurisdiction under 28 U.S.C. § 1332(d)(2) because this a proposed class action in which there are at
9 least 100 Class Members, the matter in controversy, exclusive of interest and costs, exceeds the sum
10 or value of \$5,000,000, and a member of the Class is a citizen of a different State than Defendant.

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

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

18 26. Venue properly lies in this District pursuant to 28 U.S.C. § 1391(a), (b), and (c)
19 because: a substantial part of the events or omissions giving rise to Plaintiff's and the Classes' claims
20 occurred in this District, Defendants conduct a substantial amount of business in this District, and
21 Defendants are headquartered in this District.

22 **IV. FACTUAL ALLEGATIONS**

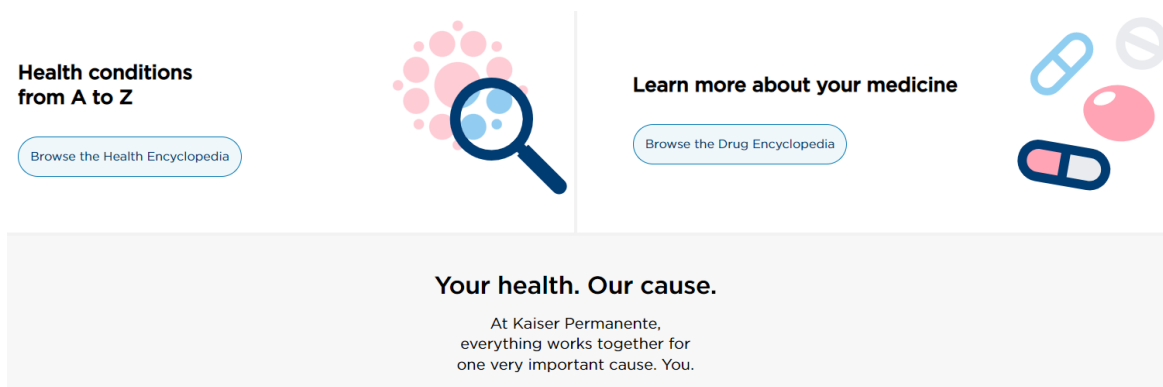
23 **A. Kaiser Permanente Communicates with Kaiser Plan Members Through the**
24 **Kaiser Permanente Website**

25 27. Plaintiff and members of the Classes are Kaiser Plan Members.

26 28. Kaiser Permanente operates a website ("Site"), with a homepage located at
27 <https://healthy.kaiserpermanente.org/front-door> ("Homepage"), through which Kaiser Plan Members
28 can perform various tasks that traditionally were only available by physically visiting their health

1 care providers’ offices or speaking directly to their health care providers, such as scheduling
2 appointments; checking medical results; reviewing medical histories; researching doctors, locations,
3 and medical services; communicating with providers and paying medical bills.


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



7
8
9
10
11
12
13
14
15 30. For example, on the Homepage, Kaiser Plan Members can click “Browse Health
16 Encyclopedia” and access a page that allows them to find health information about certain medical
17 conditions, symptoms and medical procedures, including over 4,000 health topics, by typing their
18 health-related information into a search form. Kaiser Plan Members can also check their symptoms
19 with an interactive “symptom checker” and “determine when to seek care.”
20
21
22
23
24
25
26
27
28

Search health topics

Find health information about medical conditions, symptoms, and medical procedures. Kaiser Permanente offers access to over 4,000 health topics to give you the information you need to learn the basics, get self-care, or get care from Kaiser.



Symptom checker
An interactive tool to assess health concerns and determine when to seek care.
[Check your symptoms](#)

31. 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.”

32. On the Homepage, Kaiser Plan Members can also click “Find a doctors or location” and access a form (<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.

ENTER ZIP CODE

DISTANCE

WITHIN 10 MILES
▼

OR

CITY

Select city

▼

HEALTH PLAN

Show all plans
▼

PROVIDER TYPE

Show all provider types
▼

HOSPITALS, SPECIALTIES, DOCTORS' NAMES, OR KEYWORDS

ENTER SEARCH TERMS

33. Kaiser Plan Members can also access their medical information, prescription information and test results, pay bills, schedule appointments, 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, 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>:

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

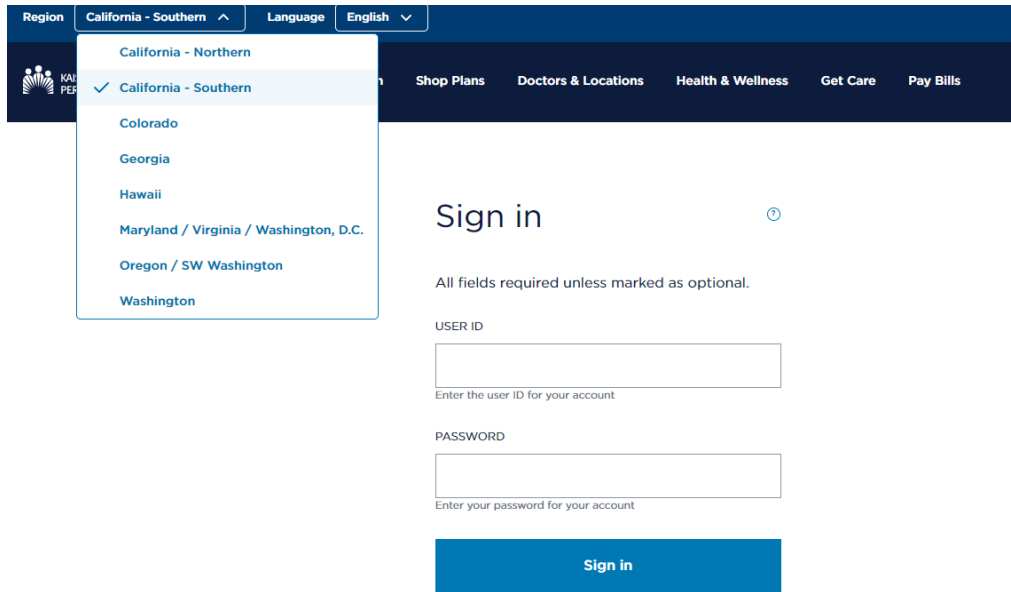
 Enter the user ID for your account

PASSWORD

 Enter your password for your account

KAISER PERMANENTE.
 We appreciate your feedback!
 Please share your experience, so we can focus on what matters to you.
[Yes, provide feedback](#)

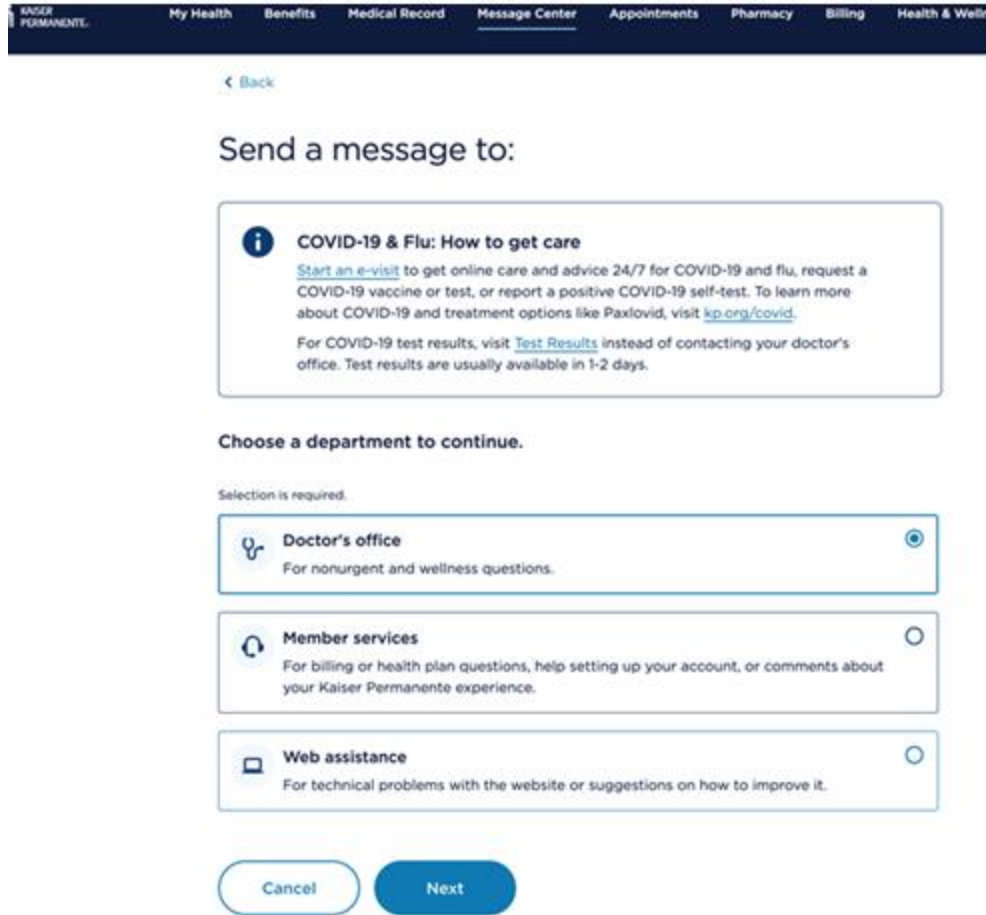
34. Kaiser Plan Members in Northern California, or other Regions such as Colorado, Georgia, Hawaii, Maryland/Virginia/Washington, D.C., Oregon/ S.W. Washington, and Washington can similarly select their region from a pulldown menu and access their Portal Login Page:



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

35. 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.

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



37. 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.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Send a message to the care team of:

Choose a recipient

What brings you here today?

Select an Option

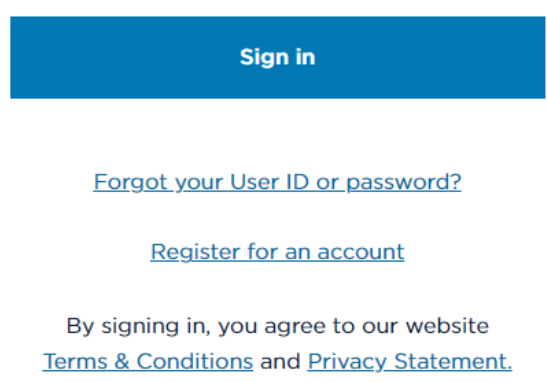
MESSAGE:

1000 of 1000 characters left

You may attach up to three files. You can send these file types: JPEG, JPG and PDF. The maximum total file size cannot exceed 4.8 megabytes.

[Get more help with attachments](#)

38. The bottom of the Portal Login Page also provides: “By signing in, you agree to our website Terms & Conditions and Privacy Statement.”



39. The Kaiser Permanente Terms & Conditions, available via hyperlink⁴ and attached hereto as Exhibit 1, provides: “Any personal information you submit to the Site (for yourself or someone else) is governed by our Website and KP Mobile Application Privacy Statement.”

⁴ See, e.g., *Terms & Conditions for our Website and Mobile Application*, Kaiser (Updated Jun. 2022), <https://healthy.kaiserpermanente.org/southern-california/termsconditions>.

1 40. The Kaiser Permanente Privacy Statement, also available via hyperlink⁵ attached
2 hereto as Exhibit 2, assures Kaiser Plan Members that Kaiser Permanente’s data collection “is
3 collected on an aggregate basis, which means that no personally identifiable information is associated
4 with the data,” which is untrue.

5 41. The Kaiser Permanente Privacy Statement also states that Kaiser Permanente and its
6 service providers may place “cookies” or similar technologies on the computer hard drives of visitors
7 to the Site, but falsely states that information obtained from cookies is only used to help Kaiser
8 Permanente “tailor our Site to be more helpful and efficient for our visitors” when in fact the cookies
9 are also being used for marketing purposes, unbeknownst to Kaiser Plan Members and without their
10 permission or agreement.

11 42. The Kaiser Permanente Privacy Statement also falsely states that “[t]he cookie
12 consists of a unique identifier that does not contain information about your health history,” when in
13 fact the information provided to the Third Party Wiretappers contains information about Kaiser Plan
14 Members’ health history.

15 43. The Kaiser Permanente Privacy Statement also states that Kaiser “may also
16 occasionally use ‘Web beacons’ (also known as ‘clear gifs,’ ‘Web bugs,’ ‘1-pixel gifs,’ etc.)” but
17 falsely claims that Kaiser Permanente does “not collect any personal health information.”

18 44. The Kaiser Permanente Privacy Statement also does not disclose to Kaiser Plan
19 Members that Kaiser Permanente has aided, agreed with, employed, and/or conspired with, third
20 parties that are recording the information that Kaiser Plan Members are sending, accessing,
21 reviewing, or receiving through the Site.

22 45. Kaiser Permanente’s website also contains a HIPAA Notice of Privacy Practices,⁶
23 which purports to describe how and when Kaiser Permanente discloses information covered by
24 HIPAA; however, nowhere in the HIPAA Notice of Privacy Practices does Kaiser Permanente
25

26 ⁵ See, e.g., *Website and mobile application Privacy Statement*, Kaiser,
27 <https://healthy.kaiserpermanente.org/southern-california/privacy> (last visited Apr. 28, 2023).

28 ⁶ See, e.g., *Notice of Privacy Practices*, Kaiser, <https://healthy.kaiserpermanente.org/southern-california/privacy-practices> (last visited Apr. 28, 2023).

1 disclose that it is providing HIPAA-protected and other confidential information to the Third Party
2 Wiretappers.

3 46. Kaiser Permanente expressly and impliedly promises Kaiser Plan Members that it will
4 maintain the privacy and confidentiality of the information shared, and the communications engaged
5 in, on the Site and the Portal and that such information and communications will not be disclosed to
6 or tracked by third parties.

7 47. Despite its express and implied assurances of privacy, Kaiser Permanente intentionally
8 incorporated the Third Party Wiretappers' code and recording technology on the Kaiser Permanente
9 website, and allowed the tracking and disclosure of Kaiser Plan Members' identifying information,
10 personal and sensitive health information, and private, sensitive, and confidential communications
11 with Kaiser Permanente and its providers to Third Party Wiretappers.

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

14 **1. Kaiser Permanente Allows Quantum Metric to Intercept Kaiser Plan**
15 **Members' Information and Communications**

16 48. Unbeknownst to Kaiser Plan Members and against their reasonable expectations,
17 Kaiser Permanents allows Quantum Metric to intercept Kaiser Plan Members' personal and sensitive
18 identifying and medical information and confidential communications from the Site and Portal.

19 49. Kaiser Permanente has placed Quantum Metric's "Session Replay" code on its
20 Homepage, Portal Login Page, and other pages on the Site—including within the Portal—which
21 intercepts and records the contents of Kaiser Plan Members' information and confidential
22 communications, and sends that information and those communications to Quantum Metric.

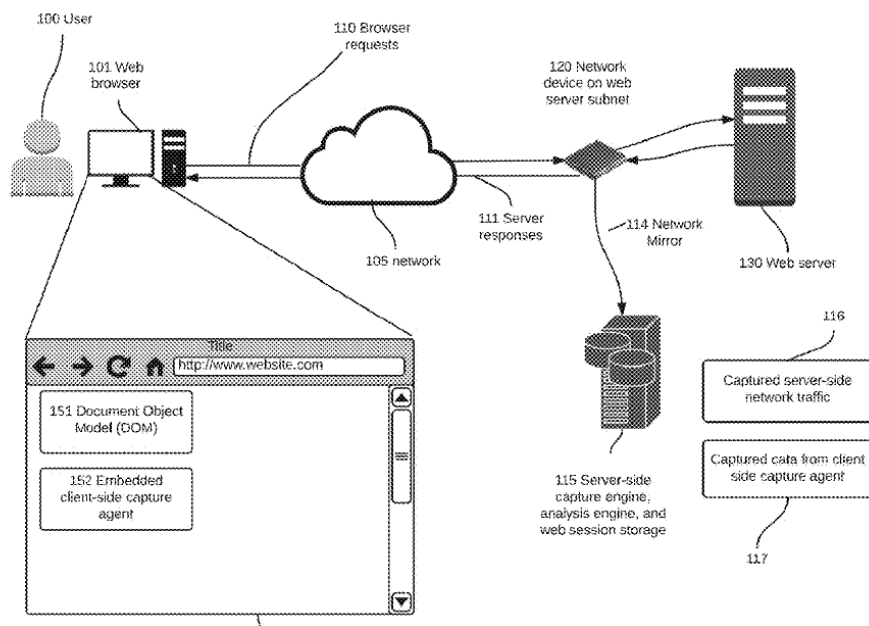
23 50. Quantum Metric collects and saves website communications, including those on the
24 Site and Portal, through a service named "Session Replay." Session Replay captures internet
25 communications between a website user and a website, including those on the Site and Portal, in real
26 time while those communications are in transit.

27 51. As Quantum Metric explains: "At its core, **session replay** is technology that allows
28 you to watch an end user's session as they experienced it, similar to how you watch a video. You can

1 pause, rewind, and fast-forward the session (just like a YouTube video) to watch how a user interacts
2 with a website or mobile app.”⁷

3 52. Session replay technologies work by using “embedded snippets of code . . . [that]
4 watch and record a visitor’s every move on a website, in real time.”⁸ This was done on the Site and
5 the Portal when used by Kaiser Plan Members.

6 53. As illustrated in Quantum Metric’s patent, after a user submits a communication to a
7 web server, such as Kaiser Permanente’s, Quantum Metric’s embedded side capture agent code
8 redirects the communications to Quantum Metric’s server-side capture engine, analysis engine, and
9 web session storage:



10
11
12
13
14
15
16
17
18
19
20
21 54. From the moment a Kaiser Plan Member loads Kaiser Permanente’s website,
22 Quantum Metric is intercepting all of the content viewed and communicated, as well as the Kaiser
23 Plan Member’s interactions with the website, similar to an individual peering over the user’s shoulder
24 and listening in on the patient’s conversations with their medical provider.

25
26
27 ⁷ *What is Session Replay*, Quantum Metric, <https://www.quantummetric.com/enterprise-guide-to-session-replay> (last visited Apr. 28, 2023).

28 ⁸ 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/>.

1 55. As Kaiser Plan Members navigate the Kaiser Permanente Site, including accessing the
2 Portal, the Site makes numerous “POST” calls to Quantum Metric, the size of which change based
3 on site activity. A “POST” call is a HTTP method that sends user data to a server.

4 56. Thus, by installing the Quantum Metric Replay code on its website, Kaiser
5 Permanente allowed Quantum Metric to intercept and record Kaiser Plan Members’ identifying
6 information, personal and sensitive medical information, including HIPAA-protected health
7 information, and confidential communications with Quantum Metric’s Session Replay code, in real
8 time.

9 57. By way of example, on April 20, 2023, after Plaintiff logged into the Portal—which
10 displayed his Name, Medical Record Number (Kaiser ID #), Region, and Coverage Status—but he
11 performed no further activities, the amount of data intercepted and transferred to Quantum Metric (at
12 kp-app.quantummetric.com) was about 16-32 bytes. Thereafter, when Plaintiff performed several
13 activities within the Portal, the amount of the data transferred to Quantum Metric increased to over
14 125kB, indicating that Plaintiff’s activity inside the Portal was being intercepted by Quantum Metric
15 and redirected to kp-app.quantummetric.com.

16 58. On April 20, 2023, after Plaintiff logged into the Portal and then accessed the Doctor
17 Search Page and performed no further activities, the amount of data intercepted and transferred to
18 Quantum Metric was 15 bytes. Thereafter, when Plaintiff entered personal medical search
19 information into the Doctor Search page, the amount of data transferred to Quantum Metric increased
20 to over 60kB, indicating that Plaintiff’s medical search information was being intercepted by
21 Quantum Metric and redirected to kp-app.quantummetric.com.

22 59. On April 20, 2023, when Plaintiff accessed the E-visit page within the Portal and
23 answered various questions as part of an E-visit mental health assessment session, the amount of data
24 transferred to Quantum Metric was over 42kB, indicating that Plaintiff’s personal information and
25 private and confidential answers to questions during the E-visit mental health assessment, were being
26 intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

27
28

1 60. On April 20, 2023, when Plaintiff accessed the Site’s health encyclopedia after
2 logging into the Portal and searched on mental health topics, the amount of data transferred to
3 Quantum Metric was over 670kB, indicating Plaintiff’s personal information and private and
4 confidential communications about mental health topics was also being intercepted by Quantum
5 Metric and redirected to kp-app.quantummetric.com.

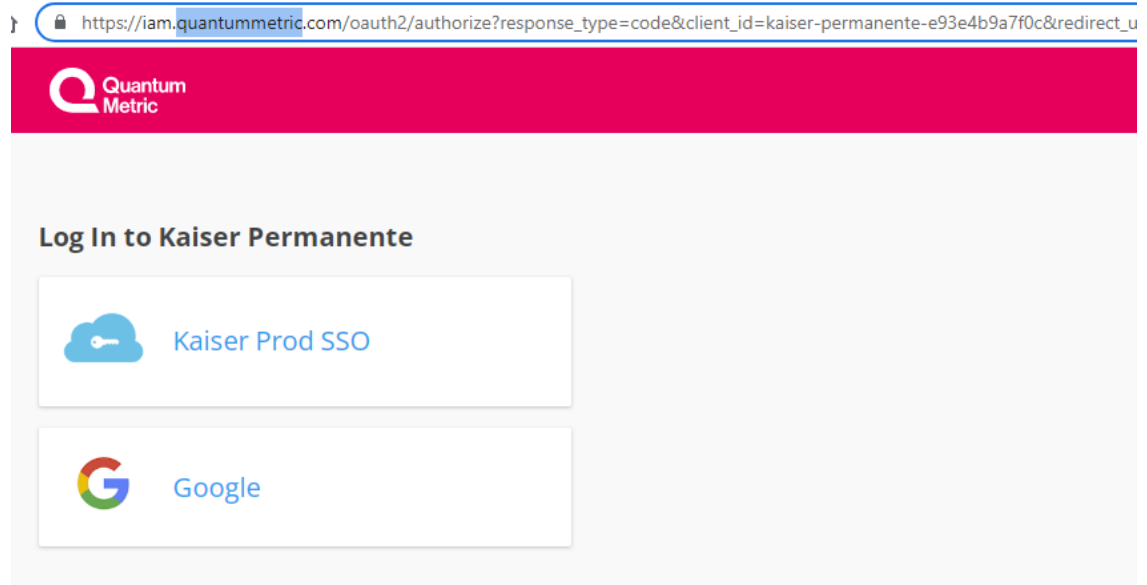
6 61. On April 21, 2023, when Plaintiff again logged into the Portal and accessed recent
7 medical test results, the amount of data transferred to Quantum Metric was over 225kB, indicating
8 that information about Plaintiff’s personal and sensitive identifying and medical information, and
9 private and confidential medical test results, was also being intercepted by Quantum Metric and
10 redirected to kp-app.quantummetric.com.

11 62. On information and belief, the same type of information tracked, disclosed, and sent
12 to Quantum Metric for Plaintiff has been tracked, disclosed, and sent to Quantum Metric for other
13 members of the Classes.

14 63. Additionally, when Kaiser Plan Members navigate other portions of the Site, Quantum
15 Metric intercepts and receives that content as well. For example, if a patient searches for doctors who
16 specialize in Addiction Medicine, Quantum Metric will receive the search results displaying this
17 sensitive information, as well as data regarding all of the information the Kaiser Plan Members
18 provided and received regarding that topic.

19 64. For example, on April 20, 2023, after Plaintiff logged-off of the Portal, Plaintiff again
20 conducted a doctor search, viewed the Homepage (Southern California region), and accessed the
21 health encyclopedia on the Site. In all cases, Plaintiff’s actions and data were intercepted by Quantum
22 Metric and transferred to kp-app.quantummetric.com.

23 65. The recordings of Plaintiff and other Class Members’ information and confidential
24 communications on the Site are saved on Quantum Metric’s systems and are available for viewing
25 on Quantum Metric’s website, an example of which is below:
26
27
28



66. Kaiser Permanente 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 Permanente and its providers.

67. Unlike certain other third parties, Quantum Metric does not only receive website analytics data that provides aggregate statistics; rather, the Quantum Metric recording technology utilized by Kaiser Permanente 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.

68. 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.

69. 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

1 recording. This may expose users [like Plaintiff and members of the Classes] to identity theft, online
2 scams, and other unwanted behavior.”⁹

3 70. The study goes on to state that “the extent of data collected by these services far
4 exceeds user expectations; text typed into forms is collected before the user submits the form, and
5 precise mouse movements are saved, all without any visual indication to the user. This data can’t
6 reasonably be expected to be kept anonymous.”¹⁰

7 71. As currently deployed, Quantum Metric’s recording function, as employed by Kaiser
8 Permanente, functions as a wiretap, and Quantum Metric acts as a third-party wiretapper.

9 **2. Kaiser Permanente Allows Adobe to Intercept Kaiser Plan Members’
10 Information and Communications**

11 72. Unbeknownst to Kaiser Plan Members and against their reasonable expectations,
12 Kaiser Permanente allows Adobe to intercept Kaiser Plan Members’ information and
13 communications from the Site and Portal.

14 73. Kaiser Permanente allows Adobe to intercept Kaiser Plan Members’ personal and
15 sensitive identifying and medical information and private and confidential communications through
16 code connected with the Adobe Experience Cloud a/k/a Adobe Marketing Cloud service embedded
17 on the Site, including within the Portal.

18 74. The Adobe Experience Cloud service is a suite of products offered by Adobe, which
19 allow businesses to personalize and improve their marketing on websites, apps, and social media
20 pages by collecting and analyzing information about website visitors.

21 75. The Adobe Experience Cloud includes a number of services including: Measurement
22 solutions, which allows companies to measure and understand visitors who use their websites, apps,
23 and social media pages, as well as how they interact with online marketing campaigns;
24 Personalization solutions, which allows companies to test new content and make their websites, apps,
25 social media pages, and emails more relevant to particular visitors; Content management solutions,

26 ⁹ Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom
27 to Tinker (Nov. 15, 2017), <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>.

28 ¹⁰ *Id.*

1 which allows companies to store, update, and deliver images and other content on their websites,
 2 within their apps, and in online marketing materials; and Advertising solutions, which allows
 3 companies to improve their online advertising on websites, apps, search engines, and social media,
 4 including helping companies send emails, text messages, and other online and offline marketing
 5 campaigns.¹¹

6 76. The Adobe Experience Cloud collects an array of information about website visitors,
 7 including:

- 8 • Where you go and what you do on that company's websites, apps, or social media
 pages
- 9 • Your web browsing activity, including the URLs of the company's web pages you
 visit
- 10 • The URL of the page that displayed the link that you clicked on, which brought you
 11 to that company's website
- 12 • The web search you performed that led you to that company's website
- 13 • Information about your web browser and device, such as device type, browser type,
 advertising identifier, operating system, connection speed, and display settings
- 14 • 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
- 15 • Location information from your mobile device or web browser
- 16 • Social media profile information
- 17 • 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
- 18 • Ad campaign success rates, such as whether you clicked on a company's ad and
 19 whether viewing or clicking on the ad led to your purchase of that company's
 product or service
- 20 • Items you've purchased or placed in your shopping cart on that company's website
 or app¹²

21 77. As part of the Adobe Advertising Cloud solution, Adobe makes available certain
 22 health-related segments supplied by third-party data providers to the companies using the Adobe
 23 Advertising Cloud, allowing companies to use these segments to target ads when they are using the
 24 Adobe Experience Cloud. These data segments generally fall into the following categories: (1)
 25 occupation in a health related field, (2) health related topics and conditions, (3) interest in health
 26

27 ¹¹ *Adobe Experience Cloud privacy*, Adobe (Updated Dec. 5, 2022), <https://www.adobe.com/privacy/experience-cloud.html>.

28 ¹² *Id.*

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

4 78. The Adobe Experience Cloud collects this information through an array of tracking
 5 technologies, including cookies and/or web beacons (also known as tags or pixels), such as the third
 6 party cookies omtrdc.net, demdex.net, and the Adobe Experience Platform Launch, which delivers a
 7 library containing specified tags for other Adobe Experience Cloud solutions.¹³

8 79. As Kaiser Plan Members navigate the Kaiser Permanente Site, the Site makes
 9 numerous “POST” calls which send information about Kaiser Plan Members’ confidential
 10 communications with Kaiser Permanente to Adobe.

11 80. Adobe has established subdomains on its own server, such as the subdomain
 12 kaiser.tt.omtrdc.net on Adobe’s omtrdc.net server, where Adobe receives and stores the
 13 communications intercepted from Kaiser Permanente.¹⁴

14 81. For example, on April 20, 2023, after Plaintiff logged into the Portal, the following
 15 data was intercepted by Adobe and sent to Adobe’s server at the kaiser.tt.omtrdc.net subdomain,
 16 which as detailed below shows that Adobe received a host of personally identifiable health
 17 information, including: user data (color coded in blue), the URL of the Website the user is currently
 18 browsing (color coded in green), unique IDs (color coded in yellow), customer IDs and status values
 19 (color coded in grey),¹⁵ and segmentation values that enable the Website to show personalized content
 20 (no color).

21 {"requestId":"107119803ed046f6b5b7a4720cb69916","context":{"userAgent":"
 22 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 23 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36","clientHints":
 24 {"mobile":false,"platform":"macOS","browserUAWithMajorVersion":"\"Chromi
 25 um\";v=\\\"112\\\", \"Google Chrome\";v=\\\"112\\\", \"Not:A-Brand\";v=\\\"99\\\""},
 26 "timeOffsetInMinutes":-420,"channel":"web","screen":{"width":3008,"height"
 27 :1692,"orientation":"landscape","colorDepth":24,"pixelRatio":2},"window":{"wi
 28 dth":1992,"height":1002},"browser":{"host":"healthy.kaiserpermanente.org","we

¹³ 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.”

¹⁴ *Adobe Experience Cloud privacy*, *supra* note 10.

¹⁵ Specific identifier number have been redacted.

bGLRenderer":"ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)","address":{"url":
 "https://healthy.kaiserpermanente.org/southern-california/secure/inner-door",
 "referringUrl":""}}, "id":{"tntId":"Redacted", "th
 irdPartyId":"15173479", "marketingCloudVisitorId":"Redacted
 ", "customerIds":[{"id":"Redacted", "integrationCode":"kpaami
 depp", "authenticatedState":"authenticated", "type":"DS"}, {"id":"Redacted", "integ
 rationCode":"kpaamidudr", "authenticatedState":"authenticated", "type":"DS"}, {"i
 d":"Redacted", "integrationCode":"kpaamid_One-off-datasets", "authenticated
 State":"authenticated", "type":"DS"}, {"id":"Redacted", "integrationCode":"pzn_cr
 m", "authenticatedState":"authenticated", "type":"DS"}, {"id":"Redacted", "integrat
 ionCode":"mbox3rdPartyId", "authenticatedState":"authenticated", "type":"DS"}]},
 "experienceCloud":{"audienceManager":{"locationHint":9, "blob":"6G1ynYcLPu
 iQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y"}, "analytics":{"logging":
 "server_side", "supplementalDataId":"Redacted
 "}}, "execute":{"pageLoad":{"parameters":{"Seg18v":"sca
 ", "Seg17v":"sca", "Seg55v":"Logged
 In", "Seg181v":"","Seg81v":"kporg:secure:inner-door", "Seg114v
 cookie":"mbr", "reEnable":"","throttle-area":"","Seg180v":false, "Seg4":true, "Seg
 517e":false, "Seg5":false, "Seg6":false, "Seg7":false, "Seg8":false, "Seg440e":false, "
 Seg9":false, "Seg11":false, "Seg20v":5579818, "Seg114v":"SUBSCRIBER", "Seg1
 3":false, "Seg14":false, "Seg16":false, "Seg19":false, "Seg516e":false, "Seg126v":fal
 se, "modval":8, "Seg21":299028, "Seg22":"https://healthy.kaiserpermanente.org/so
 uthern-california/secure/inner-door", "Seg24":"urn:kp:prodvam", "Seg25":"","enti
 tlement-446":true, "pLoaded":1, "id":""}, "profileParameters":{"region":"","Seg2":
 "54", "Seg56v":"MBR", "Seg10":"NOT ENROLLED", "Seg20v":5579818, "Seg
 12":"ACTIVE", "Seg101v":51, "Seg15":"true", "Seg106v":"KFHP_HMO", "Seg6":
 "false", "pzn_id":"Redacted", "Seg103v":false}}}, "prefetch":{"views":[{"paramet
 ers":{"Seg18v":"sca", "Seg17v":"sca", "Seg55v":"Logged In", "Seg181v":"","Seg
 81v":"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":55
 79818, "Seg114v":"SUBSCRIBER", "Seg13":false, "Seg14":false, "Seg16":false, "S
 eg19":false, "Seg516e":false, "Seg126v":false, "modval":8, "Seg21":299028, "Seg22
 ":"https://healthy.kaiserpermanente.org/southern-california/secure/inner-door",
 "Seg24":"urn:kp:prodvam", "Seg25":"","entitlement-446":true, "pLoaded":1, "id"
 :""}, "profileParameters":{"region":"","Seg2":"54", "Seg56v":"MBR", "Seg10":"N
 OT ENROLLED", "Seg20v":5579818, "Seg12":"ACTIVE", "Seg101v":51, "Seg15"
 :":true", "Seg106v":"KFHP_HMO", "Seg6":false, "pzn_id":"Redacted", "Seg103v
 ":false}}}], "telemetry":{"entries":[{"requestId":3198432, "timestamp":168201668
 5321, "execution":19.7}, {"execution":234.1, "parsing":0.1, "request":{"tls":1, "time
 ToFirstByte":218.9, "download":0.6, "responseSize":2641}, "telemetryServerToken
 ":"y6ggVo6+nhjp+nYzHbCsfoQ5YLKNHYN2xE+jRXv79rQ=", "mode":"edge", "
 features":{"executePageLoad":true, "prefetchViewCount":1, "decisioningMethod":
 "server-side"}, "requestId":"047a8d8c010a44ca959428b10b74b05d", "timestamp"
 :1682016685299}}]}

82. 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.

1 Together these details create a device fingerprint¹⁶ which allows Adobe to compile and track long-
2 term records of the individual's browsing history (and thus deliver targeted advertising or targeted
3 exploits) even when visitors are attempting to avoid tracking—raising a major concern for internet
4 privacy advocates.

5 83. The second block (green) indicates the URL for the Webpage currently visited by the
6 user. Here, Adobe is receiving information that Plaintiff has logged-into the Portal, signifying that
7 Plaintiff is a Kaiser Plan Member and Kaiser Permanente Patient—information which Kaiser
8 Permanente is prohibited from disclosing under HIPAA and other state and federal laws.

9 84. The third block (yellow) includes three identifiers set by Adobe: (1)
10 marketingCloudVisitorID, (2) tntID, and (3) thirdPartyID. These identifiers work in tandem with the
11 demdex.net server and the AMCV cookie to help specifically identify users.

12 85. When a user first visits a site with the Adobe Experience Cloud installed, like when
13 Kaiser Plan Members visit the Site and/or Portal, Adobe checks to see if the AMCV cookie is set.
14 This cookie stores the marketingCloudVisitorID (also known as Experience Cloud ID). According to
15 Adobe, the marketingCloudVisitorID “is a universal and persistent ID that identifies your visitors
16 across all solutions in the Experience Cloud.”¹⁷ In the POST called referenced above the
17 marketingCloudVisitorID is assigned a specific numeric value
18 (Redacted). This in turn allows for tracking of Kaiser Plan
19 Members across Kaiser Permanente sites and across devices.

20 86. If the AMCV cookie is not set, the Adobe code places a call to the demdex.net server,
21 which generates a marketingCloudVisitorID and sets the AMCV cookie with that value. It also sets
22 a demdex ID cookie which is persistent.¹⁸ Since the marketingCloudVisitorID is stored in the AMCV
23 cookie, it will remain the same for anyone using the browser for that specific site. When a user visits
24 another site with Adobe Experience Cloud installed, a new marketingCloudVisitorID will be
25

26 ¹⁶ Fingerprinting, web.dev, <https://web.dev/learn/privacy/fingerprinting/> (last visited Apr. 28, 2023).

27 ¹⁷ *Adobe Target Delivery API (1.0.0) Terms of Service*, Adobe, <https://developers.adobetarget.com/api/delivery-api/#section/Identifying-Visitors> (last visited Apr. 28, 2023).

28 ¹⁸ *How the Experience Cloud Identity Service requests and sets IDs*, Adobe (Updated Nov. 10, 2022), <https://experienceleague.adobe.com/docs/id-service/using/intro/id-request.html?lang=en>.

1 generated, but the demdex ID will remain the same. According to Adobe, “the demdex ID remains
2 the same . . . because it’s contained in a third-party cookie and persists across different domains.”¹⁹
3 This in turn allows Adobe to track specific devices across sites.

4 87. According to Adobe the tntID, “can be seen as a device ID.”²⁰ As detailed above,
5 device IDs use the unique setup of a user’s computer and browser to establish a device fingerprint.
6 This fingerprint can track users across various Websites to build a profile based on their Web
7 browsing habits. In the POST call referenced above the tntID is assigned a specific numeric value
8 (Redacted). The tntID is stored in the persistent mbox cookie.
9 Adobe uses the tntID as the main identifier for its Adobe Target solution.²¹ The Adobe Target system
10 is used to personalize a user’s experience on a website, like Kaiser Plan Members on the Site and
11 Portal. By default, Adobe Target captures the following data, which in turn allows the website to
12 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. ²²

21
22 88. According to Adobe, the thirdPartyID “is a persistent ID that your business utilizes to
23 identify an end-user regardless of whether they are interacting with your business from web, mobile,
24 or IoT channels. In other words, the thirdPartyId will reference user profile data that can be utilized

25
26 ¹⁹ *Id.*

²⁰ *Adobe Target Delivery API (1.0.0) Terms of Service, supra* note 15.

²¹ *Id.*

27 ²² Adapted from: *Data used by Target machine-learning algorithms*, Adobe (Updated Apr. 23, 2023),
28 <https://experienceleague.adobe.com/docs/target/using/activities/automated-personalization/ap-data.html>

1 across channels.”²³ In the POST call referenced above the thirdPartyId is assigned a specific numeric
 2 value (Redacted). This ID can be used to identify return users once they have logged into the Portal.
 3 This in turn allows Adobe’s customers to associate the thirdPartyID with a specific individual, the
 4 third party here being Kaiser Permanente’s patients.

5 89. The fourth block (grey) includes customerIds that can be, “added and associated with
 6 an Experience Cloud Visitor ID.”²⁴ In the case of the POST call above, the additional data includes
 7 the fact the user is authenticated (logged in), again signifying that Plaintiff is a Kaiser Plan Member
 8 and Kaiser Permanente patient—information which Kaiser Permanente is prohibited from disclosing
 9 under HIPAA and other state and federal laws and its express and implied contracts with Kaiser Plan
 10 Members.

11 90. Similar POST calls to kaiser.tt.omtrdc.net were found on all examined pages,
 12 including main page (Southern California), doctor search, mental health encyclopedia, e-visit, and
 13 retrieving test results.

14 91. For example, after Plaintiff logged into the Portal and accessed test results on April
 15 21, 2023, Adobe intercepted and received information about the medical procedure that Plaintiff was
 16 inquiring about, specifically a shoulder x-ray (see yellow highlight), which was transmitted to Adobe
 17 and stored on Adobe’s kaiser.tt.omtrdc.net server:

```

18 {"requestId":"d8acce0cfb0c4788ae7d98c9b6773713","context":{"userAgent":"M
19ozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
20like Gecko) Chrome/112.0.0.0 Safari/537.36","clientHints":{"mobile":false,"plat
21form":"macOS","browserUAWithMajorVersion":"\"Chromium\";v=\"112\""," \"G
22oogle Chrome\";v=\"112\""," \"Not:A-Brand\";v=\"99\""},"timeOffsetInMinutes":-
23420,"channel":"web","screen":{"width":3008,"height":1692,"orientation":"landsc
24ape","colorDepth":24,"pixelRatio":2},"window":{"width":1663,"height":1513},"
25browser":{"host":"healthy.kaiserpermanente.org","webGLRenderer":"ANGLE
26(Apple, Apple M1 Pro, OpenGL 4.1)","address":{"url":"https://healthy.kaiserpe
27rmanente.org/southern-california/secure/search-medical-record?uri=search%3a
28health-encyclopedia&type=CPT&query=73030&label=X%2DRAY+SHOULD
ER","referringUrl":"https://healthy.kaiserpermanente.org/va/inside.asp?mode=lab
detail&orderid=Redacted
"}, "id": {"tntId": "af8d349f37b54d30abbfcb86f2f2830e.35_0", "thirdPartyId": "
15173479", "marketingCloudVisitorId": "785205970708248768813052570684009
71788", "customerIds": [{"id": "Redacted", "integrationCode": "kpaamidepp", "authe
nticatedState": "authenticated", "type": "DS"}, {"id": "Redacted", "integrationCode":

```

²³ Adobe Target Delivery API (1.0.0) Terms of Service, supra note 15.

²⁴ Id.

1 "kpaamidudr","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted
 2 █","integrationCode":"kpaamid_One-off-datasets","authenticatedState":"authentic
 3 cated","type":"DS"},{"id":"Redacted █","integrationCode":"pzn_crm","authenticat
 4 edState":"authenticated","type":"DS"},{"id":"Redacted █","integrationCode":"mbo
 5 x3rdPartyId","authenticatedState":"authenticated","type":"DS"}]],"experienceClo
 6 ud":{"audienceManager":{"locationHint":9,"blob":"RKhpRz8krg2tLO6pguXWp
 7 5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y"},"analytics":{"logging":"server_sid
 8 e"},"supplementalDataId":"Redacted █"}},{"execu
 9 te":{"pageLoad":{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logg
 10 ed In","Seg181v":"","Seg81v":"kporg:secure:search-medical-record","Seg114vco
 11 okie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg
 12 517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"
 13 Seg9":false,"Seg11":false,"Seg20v":5579818,"Seg114v":"SUBSCRIBER","Seg1
 14 3":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg516e":false,"Seg126v":fal
 15 se,"modval":8,"Seg21":299028,"Seg22":"","Seg24":"urn:kp:prodvam","Seg25":"","
 16 "entitlement-446":true,"pLoaded":1,"id":""},"profileParameters":{"region":"","
 17 "Seg2":"54","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":557981
 18 8,"Seg12":"ACTIVE","Seg101v":51,"Seg15":"true","Seg106v":"KFHP_HMO","
 19 Seg6":"false","pzn_id":"Redacted █","Seg103v":false}}},"prefetch":{"views":[{"p
 20 arameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","
 21 "Seg81v":"kporg:secure:search-medical-record","Seg114vcookie":"mbr","reEn
 22 able":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5
 23 :false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11
 24 ":false,"Seg20v":5579818,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":fal
 25 se,"Seg16":false,"Seg19":false,"Seg516e":false,"Seg126v":false,"modval":8,"Seg
 26 21":299028,"Seg22":"","Seg24":"urn:kp:prodvam","Seg25":"","entitlement-446"
 27 :true,"pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"54","Seg56v
 28 v":"MBR","Seg10":"NOT ENROLLED","Seg20v":5579818,"Seg12":"ACTIVE"
 29 ,"Seg101v":51,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id"
 30 :Redacted █,"Seg103v":false}}},"telemetry":{"entries":[{"requestId":3198432,"
 31 timestamp":1682104634267,"execution":13.8},{ "execution":56,"parsing":0.1,"re
 32 quest":{"tls":0.9,"timeToFirstByte":49.7,"download":0.7,"responseSize":1565},"t
 33 elemetryServerToken":"GRgdNPKF2baxcRHAQqAHqyTPswyQefSCMFGH9G
 34 Y2aUI=","mode":"edge","features":{"executePageLoad":true,"prefetchViewCoun
 35 t":1,"decisioningMethod":"server-
 36 side"},"requestId":"a241e476537c46ee889a2bd5
 37 ea8970a2","timestamp":1682104634251}}]}

20 92. On April 20, 2023, when Plaintiff was logged out of the Portal and conducted a search
 21 on the Site's encyclopedia page for mental health, Adobe intercepted and received the following data
 22 (highlighted in yellow), which includes the various personal IDs detailed above (such as Plaintiff's
 23 tntID and marketingCloudVisitorID) and discloses the fact that Plaintiff had requested information
 24 from Kaiser Permanente regarding "mental health," which was transmitted to Adobe and stored on
 25 Adobe's kaiser.tt.omtrdc.net server:

26 {"requestId":"ce17897a88f94df8911b81e1dbf35ecd","context":{"userAgent":"M
 27 ozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
 28 like Gecko) Chrome/112.0.0.0 Safari/537.36","clientHints":{"mobile":false,"plat
 form":"macOS","browserUAWithMajorVersion":"\"Chromium\";v=\"112\""," \"Go
 ogle Chrome\";v=\"112\""," \"Not:A-Brand\";v=\"99\""},"timeOffsetInMinutes":-

420,"channel":"web","screen":{"width":3008,"height":1692,"orientation":"landscape","colorDepth":24,"pixelRatio":2},"window":{"width":1992,"height":1357},"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=mental+health&category=global&global-region=sca&language=english®ion=sca"},"referringUrl":"https://healthy.kaiserpermanente.org/southern-california/health-wellness/health-encyclopedia"}}, "id":{"tntId":"Redacted"}, "marketingCloudVisitorId":"Redacted", "experienceCloud":{"audienceManager":{"locationHint":9,"blob":"RKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"Redacted"}}, "execute":{"pageLoad":{"parameters":{"Seg18v":"sca","Seg17v":"","Seg55v":"Logged Out","Seg181v":"","Seg81v":"kporg:pages:search","Seg114vcookie":"","reEnable":"","throttle-area":""},"profileParameters":{"region":"","Seg2":"54"}}, "prefetch":{"views":[{"parameters":{"Seg18v":"sca","Seg17v":"","Seg55v":"Logged Out","Seg181v":"","Seg81v":"kporg:pages:search","Seg114vcookie":"","reEnable":"","throttle-area":""},"profileParameters":{"region":"","Seg2":"54"}]}]}, "telemetry":{"entries":[{"requestId":3198432,"timestamp":1682019482663,"execution":20.9}, {"requestId":203,"timestamp":1682019482663,"execution":20.9}, {"requestId":0.1,"timestamp":1682019482663,"execution":20.9}, {"requestId":1.2,"timestamp":1682019482663,"execution":20.9}, {"requestId":196.8,"timestamp":1682019482663,"execution":20.9}, {"requestId":0.3,"timestamp":1682019482663,"execution":20.9}, {"requestId":1842,"timestamp":1682019482663,"execution":20.9}], "telemetryServerToken":"sWzAuPN0jRUiKvgomAHTp5Xnsnn8TJkKAI00wNaSyq4=", "mode":"edge", "features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},"requestId":"90b30902cc1a457bbbf75df338f3a4d6","timestamp":1682019482638}}}

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

3. Kaiser Permanente Allows Twitter, Bing, and Google to Intercept Patients' Communications

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

95. Google and Bing are the most widely used search engines, and Twitter is one of the largest social media sites in the world.

96. Generally, Google, 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.

97. 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

1 valuable to Twitter because it helps advertisers understand who Twitter users are so that Twitter can
2 sell advertisements targeting that particular user’s Twitter timelines.²⁵

3 98. Twitter also tracks browsing activity outside of Twitter, for both Twitter users and
4 people who have never created an account on the Twitter platform, including browser type, the device
5 and operating system, the mobile carrier, IP address, and browsing activity.²⁶ Twitter can also learn
6 information about websites visited before landing on the referring website and what websites were
7 visited after leaving the site.²⁷

8 99. Google and Bing sell ads based on a user’s search. So, a search for a medical condition
9 such as cancer, would show ads for cancer treatment centers.

10 100. Google and Bing are also widely used ad platforms that provide ad remarketing.
11 Remarketing shows ads based on sites a user has previously visited. For example, a user who visits a
12 website with Google or Bing code, and searches on pregnancy related topics, might then see ads for
13 a Google or Bing advertiser’s pregnancy related services on other websites.

14 101. A main goal for Google, Bing, and Twitter is to develop a profile of users to better
15 target them with ads. Therefore, all these sites offer free analytics tools. These tools are useful to
16 advertisers as they can show how effective certain ads are. Web analytics tools also provide general
17 information about who is visiting the website and what those users are doing on the site.

18 102. The Kaiser Permanente Site, including inside the Portal, uses Bing Ads and Google
19 and Twitter analytics. The Kaiser Permanente Website, including inside the Portal, also tracks views
20 via integration with Doubleclick, which is owned by Google.

21 103. Bing, Google, and Twitter send data to their respective servers via HTTP GET request
22 parameters.

23 104. The HTTP GET method requests data from a server. This request can include
24 additional parameters that are sent as part of the request URL. For example, take the request
25 “www.example.com ?utm_source=google.” In this case, everything after the “?” is used to track

26 ²⁵ Mehak Siddiqui, *What Does Twitter Know About Me?*, vpnoverview (Sept. 9, 2022),
27 <https://vpnoverview.com/privacy/social-media/what-does-twitter-know-about-me/>.

²⁶ *Id.*

²⁷ *Id.*

1 where the site visitor came from, in this case showing that the visitor came from Google before
2 accessing the www.example.com.

3 **a) Portal Login**

4 105. On April 20, 2023, when Plaintiff logged into the Portal, Bing sent the following GET
5 request to bat.bing.com (color coded here and described in more detail below):

6 <https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=1ae9f073-60a4-44f7-bce9-43d2cf4488fe&sid=294d9520dfab11edaa7d1755dd644c7f&vid=294dbe90dfab11ed9ef7ad76fb5ac623&vids=0&msclkid=N&pi=9Redacted&lg=en-US&sw=3008&sh=1692&sc=24&tl=My%20Health%20%7C%20Kaiser%20Permanente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&r=<=529&evt=pageLoad&sv=1&rn=447477>

7
8
9
10 106. The Bing GET request includes temporary and session IDs (mid, sid, vid)—
11 highlighted in yellow above, an indication that the page loaded (green highlight), the URL of the page
12 (blue highlight), information about the browser and device (grey highlight) and a hash (pi) (pink
13 highlight)—of the device data. As discussed above, hashes such as this are used to establish a device
14 fingerprint to track devices across multiple websites. The data sent to Bing indicates the user
15 successfully logged into the Portal.

16 107. According to Bing documentation, “the cookie in the relevant domain and IP address
17 are always passed with every http request and not just via UET.”²⁸ UET is Universal Event Tagging
18 and it’s the method used by Bing to report advertiser activity on a Website. UET was installed on all
19 pages viewed on the Kaiser Website, including within the Portal.

20 108. When Plaintiff logged into the Portal, Google also sent multiple GET requests to both
21 googleads.g.doubleclick.net and google.com. These requests are essentially similar in nature. For
22 example, the data sent via GET to Google servers at googleads.g.doubleclick.net is below:

23 https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1682016746120&cv=11&fst=1682016746120&bg=ffffff&guid=ON&asyn=1>m=45be34c0&u_w=3008&u_h=1692&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&labeled=Ump9CM7hr3IQosSlpAM&hn=www.googleadservices.com&frm=0&tiba=My%20Health%20%7C%20Kaiser%20Permanente&auid=1394501439.1682016175&uaa=arm&uab=64&uafvl=Chromium%3B112.0.5615.137%7CGoogle%2520Chrome%3B112.0.5615.137%7CNot%253AA-Brand%3B99.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event%3Dconversion&rfmt=3&fmt=4

28 ²⁸ <https://help.ads.microsoft.com/apex/index/3/en/53056/>

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

5 110. When Plaintiff logged into the Portal, Google used the POST method to transmit the
6 following data to Google servers at www.google-analytics.com:

7 https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70>m=45je34c0&_p=941729214&cid=1604752619.1682016174&ul=en-us&sr=3008x1692&uaa=arm&uab=64&uafvl=Chromium%3B112.0.5615.137%7CGoogle%2520Chrome%3B112.0.5615.137%7CNot%253AA-Brand%3B99.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&_s=3&sid=1682016174&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-sign-on&dt=My%20Health%20%7C%20Kaiser%20Permanente&en=user_engagement&_et=8100

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

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

20 https://analytics.twitter.com/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=b7251997-28cf-4dcc-9926-53d9a01ba6c1&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=bb45caa1-c7d9-4d71-893c-b875d9fef676&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

23 113. As reflected above, highlighted in blue, the Twitter GET requests were used to indicate
24 a page view of the Portal—indicating the user successfully logged in.

25 **b) Inside the Portal—Accessing Test Results**

26 114. On April 21, 2023, when Plaintiff accessed test results from within the Portal, Bing,
27 Google, and Twitter all transmitted the fact that Plaintiff has a shoulder X-ray in their GET requests
28 back to their respective servers.

1 115. For example, Bing's GET request from the test results page was:

2 <https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=6fff0767-39ee-4add-b2c8-400f112dd65b&sid=294d9520dfab11edaa7d1755dd644c7f&vid=294d-be90dfab11ed9ef7ad76fb5ac623&vids=0&msclkid=N&pi=9Redacted &lg=en-US&sw=3008&sh=1692&sc=24&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%2Fva%2Finside.asp%3Fmode%3Dlabdetail%26orderid%3DWP-24V-2B3NQ2bC6-2BleBI3Fg9nA2psYu22GNxSPpkW8KgU5hKk-3D-24RP2b0miWDEm9WTRBUztJc9Ww7w1Jn-2FJdxlN-2BDlvTwmJ-3D<=759&evt=pageLoad&sv=1&rn=152034>

3
4
5
6
7
8 116. The 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), information about the browser and device (grey highlight) and the same hash (pi) as the Portal (pink highlight), which identifies the computing device and allows for long term tracking. The GET request also transmitted to Bing, the URL of the page (blue highlight), which in this case also includes the fact that Plaintiff had a shoulder X-ray. This data can be used to better target ads.

9
10
11
12
13
14 117. Doubleclick's (and Google.com which was essentially similar) GET request from the test results page was:

15
16 https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1682104687968&cv=11&fst=1682104687968&bg=ffffff&guid=ON&asyn=1>m=45be34j0&u_w=3008&u_h=1692&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fmedical-record%2Ftest-results&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DCPT%26query%3D73030%26label%3DX%252DRAY%2BSHOULDER&label=Ump9CM7hr3IQosSlpAM&hn=www.googleadservices.com&frm=0&tiba=Test%20Results%20%7C%20Medical%20Record%20%7C%20Kaiser%20Permanente&auid=202926121.1682019380&uaa=arm&uab=64&uafvl=Chromium%3B112.0.5615.137%7CGoogle%2520Chrome%3B112.0.5615.137%7CNot%253AA-Brand%3B99.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event%3Dconversion&rfmt=3&fmt=4

17
18
19
20
21
22 118. The above GET request includes data about the browser and device (grey highlight) and an indication the page loaded (green highlight). The URL of the page (blue highlight) reveals Plaintiff had a shoulder X-ray. This data can be used to better target ads.

23
24
25 119. While Plaintiff was accessing the test results page, Google also used the POST method to transmit the following data to Google servers at www.google-analytics.com:

26
27 https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70>m=45je34j0&_p=1450148043&cid=1038125726.1682019380&ul=en-us&sr=3008x

1 1692&uaa=arm&uab=64&uafvl=Chromium%3B112.0.5615.137%7CGoogle%25
 2 20Chrome%3B112.0.5615.137%7CNot%253AA-Brand%3B99.0.0.0&uamb
 3 =0&uam=&uap=macOS&uapv=13.3.1&uaw=0&sid=1682104236&sct=2&seg=1
 4 &dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california
 5 %2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-
 6 encyclopedia%26type%3DCPT%26query%3D73030%26label%3DX%252DRAY%2BSHOULDER&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fva
 7 %2Finside.asp%3Fmode%3Dlabdetail%26orderid%3DRedacted
 8 Redacted &dt=Search%20medical%20
 9 records&_s=1

10 120. The POST above includes temporary and session IDs (tid, cid, sid)—highlighted in
 11 yellow, and information about the browser and device (grey highlight). The URL of the current page
 12 (blue highlight) reveals Plaintiff’s shoulder X-ray. The data sent to Google can be used to better target
 13 ads.

14 121. Twitter’s (both analytics.twitter.com and t.co) GET request from the test results page
 15 was:

16 https://analytics.twitter.com/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=
 17 06866b4e-da1b-4d15-a234-850bb5ed9e0b&integration=advertiser&p_id=Twitter
 18 &p_user_id=0&pl_id=130452a7-272c-49f6-9af1-582495f6cefc&tw_document_
 19 href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california
 20 %2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclo
 21 pedia%26type%3DCPT%26query%3D73030%26label%3DX%252DRAY%2BSH
 22 OULDER&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

23 122. The Twitter GET requests reveal in the current site URL (highlighted in blue) that
 24 plaintiff had a shoulder X-ray. This data can be used to better target ads, in this case showing a
 25 shoulder injury so that Plaintiff could be targeted for such things as shoulder slings and physical
 26 therapy services.

27 c) Other Searches on the Site

28 123. On April 20, 2023 while logged out of the Portal, Plaintiff accessed Kaiser’s Health
 Encyclopedia and searched on Mental Health. On the search results page, Bing sent the following
 GET request:

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=ce46f37b-ee7d-47c6-
 975a-6eba4dae3726&sid=294d9520dfab11edaa7d1755dd644c7f&vid=2
 94dbe90dfab11ed9ef7ad76fb5ac623&vids=0&mssclkid=N&pi=9Redacted &lg=e
 n-US&sw=3008&sh=1692&sc=24&tl=Search%20%7C%20Kaiser%20Perman
 ente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california
 %2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%
 26global-region%3Dsc%26language%3Denglish%26region%3Dsc&r=https%3

1 A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-well
2 ness%2Fhealth-encyclopedia<=1069&cv=pageLoad&sv=1&rn=167058

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

10 125. Doubleclick's (and Google.com which was essentially similar) GET request from the
11 mental health search results page was:

12 https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1682019177873&cv=11&fst=1682019177873&bg=ffffff&guid=ON&async=1>m=45be34j0&u_w=3008&u_h=1692&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-wellness%2Fhealth-encyclopedia&label=Ump9CM7hr3IQoSslpAM&hn=www.googleadservices.com&frm=0&tiba=Search%20%7C%20Kaiser%20Permanente&auid=883163547.1682018211&uaa=arm&uab=64&uafvl=Chromium%3B112.0.5615.137%7CGoogle%2520Chrome%3B112.0.5615.137%7CNot%253AA-Brand%3B99.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event%3Dconversion&rfmt=3&fmt=4

13 126. The above GET request includes data about the browser and device (grey highlight)
14 and an indication the page loaded (green highlight). The URL of the page (blue highlight) reveals
15 Plaintiff searched on the term "mental health." This data can similarly be used to better target ads.
16

17 127. When Plaintiff conducted a search for "mental health", Google used the POST method
18 to transmit the following data to Google servers at www.google-analytics.com:

19 https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70>m=45je34j0&_p=247229106&cid=359940215.1682018211&ul=en-us&sr=3008x1692&uaa=arm&uab=64&uafvl=Chromium%3B112.0.5615.137%7CGoogle%2520Chrome%3B112.0.5615.137%7CNot%253AA-Brand%3B99.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&_s=2&sid=1682018210&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-wellness%2Fhealth-encyclopedia&dt=Search%20%7C%20Kaiser%20Permanente&en=user_engagement&_et=9825

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

5 129. Twitter’s (both analytics.twitter.com and t.co) GET request from the mental health
6 search results page was:

7 https://analytics.twitter.com/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=ea2c59e7-c242-4c28-bf04-90aac0c1ab15&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=8b91e4f2-13e0-4d37-9550-913dade83cbb&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%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

10 130. The Twitter GET request in the current site URL (highlighted in blue) reveals that
11 Plaintiff searched on the term “mental health.” This data can similarly be used to better target ads.

12 131. On information and belief, the same type of information tracked, disclosed, and sent
13 to Bing, Google, and Twitter for Plaintiff has been tracked, disclosed, and sent to Bing, Google, and
14 Twitter for other members of the Classes.

15 132. Whenever Kaiser Plan Members use Kaiser Permanente’s website, Kaiser Permanente
16 allows Bing, Google, and Twitter to intercept the contents of their communications—including
17 personal information, identifying information, and sensitive medical information—without their
18 knowledge, consent, or authorization.

19 133. Kaiser Permanente knowingly redirects and discloses Kaiser Plan Members’
20 personally identifiable patient data, including their status as patients and the contents of their
21 communications with Kaiser Permanente to Bing, Google, and Twitter.

22 134. Despite its legal obligations to keep this information and these communications
23 private and confidential, Kaiser Permanente’s use of Bing, Google, and Twitter analytics causes the
24 redirection, interception, and transmission of the precise content of patients’ communication with
25 Kaiser Permanente to Bing, Google, and Twitter.

26 135. Kaiser Permanente’s unauthorized redirection and disclosures to Bing, Google, and
27 Twitter includes information that identifies Plaintiff and Class Members as patients of Kaiser
28

1 Permanente, and aids in receiving and recording patient communications pertaining to or about
2 specific medical conditions, health services, and specific doctors.

3 136. Kaiser Permanente's disclosures to Bing, Google, and Twitter occur because Kaiser
4 Permanente intentionally deploys Bing, Google, and Twitter code on its website, and that code
5 commandeers Kaiser Plan Members' web-browsers and causes personally identifiable patient data,
6 as well as the contents of communications exchanged between Kaiser Permanente and its patients, to
7 be redirected and sent to Bing, Google, and Twitter.

8 137. As currently deployed, Bing, Google, and Twitter analytics, as employed by Kaiser
9 Permanente, functions as a wiretap, and Bing, Google, and Twitter as third-party wiretappers.

10 **C. Plaintiff and Class Members Did Not Consent to Kaiser Permanente Disclosure**
11 **of Their Information and Communications to Third Parties**

12 138. Kaiser Permanente does not ask Kaiser Plan Members who use its Site and Portal,
13 including Plaintiff, whether they consent to having the contents of their information and
14 communications with Kaiser Permanente disclosed to the Third Party Wiretappers. Kaiser Plan
15 Members are never actively told that their electronic communications are being wiretapped by Third
16 Party Wiretappers.

17 139. Kaiser Permanente states in its Privacy Policy, under the heading "Internet Cookies,"
18 that:

19 We and our service providers *may* place Internet "cookies" or similar technologies
20 (JavaScript, HTML5, ETag) on the computer hard drives of visitors to the Site.
21 Information we obtain helps us to tailor our Site to be more helpful and efficient
22 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.

23 Website and mobile application Privacy Statement, Kaiser, <https://healthy.kaiserpermanente.org>
24 /privacy (last visited May 3, 2023) (emphasis added).

25 140. This does not disclose that Kaiser Permanente sends Plaintiff's and Class Members'
26 information and communications to the Third Party Wiretappers.

27 141. First, these "third parties" are not defined in the Website Privacy Policy.
28

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

3 143. Third, Kaiser Permanente falsely claims that information about Kaiser Plan Members’
4 health history is not being transmitted.

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

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

15 **D. Plaintiff’s and Class Members’ Health Information Has Actual, Measurable,
16 Monetary Value**

17 146. Kaiser Plan Members’ confidential communications and information that Kaiser
18 Permanente allows the Third Party Wiretappers to intercept has monetary value.

19 147. For example, one recent study asked over a thousand consumers from around the
20 world what price they would demand of third parties for access to their data and found that passwords
21 would fetch \$75.80; health information and medical records themselves average \$59.80; and in third,
22 Social Security numbers were valued at \$55.70.²⁹

23 148. Some companies, such as Prognos Health, sell what they purport to be de-identified
24 health information from millions of patients.³⁰

25 _____
26 ²⁹ Jonathan Weicher, *Healthcare hacks—how much is your personal information worth?*, Netlib
27 Security, [https://netlibsecurity.com/articles/healthcare-hacks-how-much-is-your-personal-informati
28 on-worth/](https://netlibsecurity.com/articles/healthcare-hacks-how-much-is-your-personal-information-worth/) (last visited Apr. 28, 2023).

³⁰ 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](https://prognoshealth.com/about-us/news/press-release/prognos-health-announces-patent-pending-technology).

1 149. Due to the difficulty in obtaining health information, illegal markets also exist for such
2 data, with some reporting that health data can be “more expensive than stolen credit card numbers.”³¹

3 **E. Kaiser Permanente’s Conduct Violates State and Federal Privacy Laws**

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

11 151. Plaintiff and Class Members reasonably believed their interactions with Kaiser
12 Permanente on the Site and Portal were private and would not be transmitted to third parties, recorded,
13 or monitored for a later playback.

14 152. The data collected by Kaiser Permanente identified specific web pages navigated and
15 content viewed, and thus revealed personalized and sensitive information about Plaintiff and Class
16 Members, including sensitive personal and medical information.

17 153. Plaintiff and Class Members did not have a reasonable opportunity to discover
18 Defendants’ unlawful and unauthorized connections and conduct because Kaiser Permanente did not
19 disclose its actions nor seek consent from Plaintiff or Class Members prior to making the
20 transmissions to third parties.

21 154. Privacy polls and studies uniformly show that the overwhelming majority of
22 Americans consider one of the most important privacy rights to be the need for an individual’s
23 affirmative consent before a company collects and shares its customers’ personal data.

24
25
26
27 ³¹ Aarti Shahani, *The Black Market For Stolen Health Care Data*, NPR (Feb. 13, 2015, 4:55 am),
28 <https://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data>.

1 155. For example, a study by Pew Research Center indicated that an overwhelming
2 majority of Americans—approximately 79%—are concerned about how data is collected about them
3 by companies.³²

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

8 157. Plaintiff’s and Class Members’ reasonable expectation of privacy in their personally
9 identifiable data and communications exchanged with Kaiser Permanente and its providers is derived
10 from several sources, including:

- 11 a. Kaiser Permanente’s status as Kaiser Plan Members’ health care provider;
- 12 b. Kaiser Permanente’s common law obligation to maintain confidentiality of
13 patient data and communications;
- 14 c. State and federal laws and regulations protecting the confidentiality of medical
15 information;
- 16 d. State and federal laws protecting the confidentiality of communication and
17 computer data;
- 18 e. Defendants’ express promises of privacy and confidentiality; and
- 19 f. Defendants’ implied promises of privacy and confidentiality.

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

22 159. The HIPAA Privacy Rule, located at 45 CFR § 160 and Subparts A and E of § 164,
23 “establishes national standards to protect individuals’ medical records and other individually
24 identifiable health information (collectively defined as ‘protected health information’) and applies to
25

26 ³² Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control*
27 *Over Their Personal Information*, Pew Research Center (Nov. 15, 2019),
28 <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

1 health plans, health care clearinghouses, and those health care providers that conduct certain health
2 care transactions electronically.”³³

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

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

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

18 163. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: “(1)
19 uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health
20 information relating to an individual.” 42 U.S.C. § 1320d-6. The statute states that a “person . . . shall
21 be considered to have obtained or disclosed individually identifiable health information . . . if the
22 information is maintained by a covered entity . . . and the individual obtained or disclosed such
23 information without authorization.” *Id.*

24 164. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to
25 Kaiser Permanente when it knowingly disclosed individually identifiable health information relating
26 to an individual, as those terms are defined under HIPAA.

27 _____
28 ³³ *The HIPAA Privacy Rule*, HHS, <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> (last visited Apr. 28, 2023).

1 165. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-
2 6(b). There is a penalty enhancement where “the offense is committed with intent to sell, transfer, or
3 use individually identifiable health information for commercial advantage, personal gain, or
4 malicious harm.” *Id.* In such cases, the entity that knowingly obtains individually identifiable health
5 information relating to an individual shall “be fined not more than \$250,000, imprisoned not more
6 than 10 years, or both.” *Id.*

7 166. Guidance from HHS confirms that patient status is protected by HIPAA, which
8 provides

9 Identifying information alone, such as personal names, residential addresses, or
10 phone numbers, would not necessarily be designated as PHI. For instance, if such
11 information was reported as part of a publicly accessible data source, such as a
12 phone book, then this information would not be PHI because it is not related to
13 health data. . . . ***If such information was listed with health condition, health care
14 provision or payment data, such as an indication that the individual was treated
15 at a certain clinic, then this information would be PHI.***³⁴

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

18 The HIPAA Privacy Rule gives individuals important controls over whether and
19 how their protected health information is used and disclosed for marketing
20 purposes. With limited exceptions, the Rule requires an individual’s written
21 authorization before a use or disclosure of his or her protected health information
22 can be made for marketing. . . . Simply put, a covered entity may not sell protected
23 health information to a business associate or any other third party for that party’s
24 own purposes. **Moreover, covered entities may not sell lists of patients or
25 enrollees to third parties without obtaining authorization from each person on
26 the list.**³⁵

27 168. HHS has previously instructed that patient status is protected by the HIPAA Privacy
28 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

³⁴ *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 (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/Deidentification/hhs_deid_guidance.pdf. (emphasis added) (last visited Apr. 28, 2023).

³⁵ *Marketing* at 1-2, Office for Civil Rights (Rev. Apr. 3, 2003), <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/marketing.pdf>. (emphasis added).

1 includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186
2 (Aug. 14, 2002);

3 c. It would be a HIPAA violation “if a covered entity impermissibly disclosed a list
4 of patient names, addresses, and hospital identification numbers.” 78 Fed. Reg.
5 5642 (Jan. 25, 2013); and

6 d. The only exception permitting a hospital to identify patient status without express
7 written authorization is to “maintain a directory of individuals in its facility” that
8 includes name, location, general condition, and religious affiliation when used or
9 disclosed to “members of the clergy” or “other persons who ask for the individual
10 by name.” 45 C.F.R. § 164.510(1). Even then, patients must be provided an
11 opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R.
12 § 164.510(2).

13 **V. TOLLING**

14 169. Plaintiff repeats and incorporates all other paragraphs as if fully set forth herein.

15 170. The statutes of limitations applicable to Plaintiff’s and the Classes’ claims were tolled
16 by Defendants’ conduct and Plaintiff’s and Class Members’ delayed discovery of their claims.

17 171. As alleged above, Plaintiff and members of the Classes did not know and could not
18 have known when they used the Kaiser Permanente Site and/or Portal that Kaiser Permanente was
19 disclosing their information and communications to third parties. Plaintiff and members of the Classes
20 could not have discovered Kaiser Permanente’s unlawful conduct with reasonable diligence.

21 172. Kaiser Permanente secretly incorporated the Third Party Wiretappers’ code into the
22 Site, including the Portal, providing no indication to Kaiser Plan Members and Site users that their
23 communications would be disclosed to these third parties.

24 173. Kaiser Permanente had exclusive and superior knowledge that the Third Party
25 Wiretappers’ code incorporated on its Site would disclose Kaiser Plan Members’ protected and
26 private information and confidential communications, yet failed to disclose to Kaiser Plan Members
27 and Site users that by interacting with the Kaiser Permanente Site and/or Portal that Plaintiff’s and
28 Class Members’ patient status, personal information, sensitive health information, and confidential
communications would be disclosed to third parties.

174. Plaintiff and Members of the Classes could not with due diligence have discovered the
full scope of Kaiser Permanente’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

1 reasonable consumer or Site user that Kaiser Permanente was disclosing and allowing the interception
2 of such information to these third parties.

3 175. The earliest Plaintiff and Class Members could have known about Defendants’
4 conduct was shortly before the filing of this Complaint.

5 **VI. CLASS ACTION ALLEGATIONS**

6 176. Plaintiff brings this action pursuant to Federal Rules of Civil Procedure 23(a) and
7 23(b)(2) and/or (b)(3) on behalf of the following Class and Sub-Classes:

8 **Nationwide Class:** All Kaiser Plan Members in the United States who used the
9 Kaiser Permanente website.

10 **California Sub-Class:** All Kaiser Plan Members who are residents of the State of
11 California and used the Kaiser Permanente website.

12 **Nationwide Breach of Contract Sub-Class:** All Kaiser Plan Members who used
13 the Portal on the Kaiser Permanente website.

14 **California Breach of Contract Sub-Class:** All Kaiser Plan Members who are
15 residents of the State of California and used the Portal on the Kaiser Permanente
16 website.

17 177. Excluded from the Class and Sub-Class are Defendants and their parents, subsidiaries,
18 and corporate affiliates. Plaintiff reserves the right to revise the definition of the Class and Sub-Class
19 based upon subsequently discovered information and reserves the right to establish additional Sub-
20 Class where appropriate. The Class and Sub-Class are collectively referred to herein as the “Class”
21 or “Classes.”

22 178. The Classes are so numerous that joinder of all members is impracticable. Plaintiff
23 believes that there are at least tens of thousands of proposed members of the Classes throughout the
24 United States.

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

- 28 • 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.*;

- 1 • Whether Defendants' acts and practices violated California's Constitution, Art. 1, § 1;
- 2 • Whether Defendants' acts and practices violations Plaintiff's and Class Members' common law privacy rights;
- 3 • Whether Defendants breached a express contract;
- 4 • Whether Defendants breached an implied contract; and
- 5 • Whether damages, restitution, equitable, injunctive, compulsory, or other relief is warranted.

6
7 180. Plaintiff's claims are typical of the claims of the Class that Plaintiff seeks to represent.
8 As alleged herein, Plaintiff and the Class sustained damages arising out of the same unlawful actions
9 and conduct by Defendants.

10 181. Plaintiff is willing and prepared to serve the Class in a representative capacity with all
11 of the obligations and duties material thereto. Plaintiff will fairly and adequately protect the interests
12 of the Class and has no interest adverse to or in conflict with the interests of the other members of the
13 Class.

14 182. Plaintiff's interests are co-extensive with and are not antagonistic to those of absent
15 members within the Class. Plaintiff will undertake to represent and protect the interests of absent
16 members within the Class and will vigorously prosecute this action.

17 183. Plaintiff has engaged the services of the undersigned counsel. Counsel is experienced
18 in complex litigation, will adequately prosecute this action and will assert and protect the rights of,
19 and otherwise represent, Plaintiff and absent members of the Class.

20 184. A class action is superior to all other available methods for the fair and efficient
21 adjudication of this controversy. Plaintiff knows of no difficulty to be encountered in the management
22 of this litigation that would preclude its maintenance as a class action.

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

27 186. The Class may also be certified under Federal Rule of Civil Procedure 23(b)(2)
28 because Defendants have acted on grounds generally applicable to the Classes, thereby making it

1 appropriate to award final injunctive relief or corresponding declaratory relief with respect to the
2 Classes.

3 187. The interest of members within the Class individually controlling the prosecution of
4 separate actions is theoretical and not practical. The Classes have a high degree of similarity and are
5 cohesive, and Plaintiff anticipates no difficulty in the management of this matter as a class action.

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

10 **VII. CLAIMS FOR RELIEF**

11 **FIRST CLAIM FOR RELIEF**
12 **Violation of the Electronic Communications Privacy Act, 18 U.S.C §§ 2510, *et seq.***
13 **(On Behalf of the Nationwide Class)**

14 189. Plaintiff repeats and incorporates all other paragraphs as if fully set forth herein.

15 190. Plaintiff brings this claim individually and on behalf of the Nationwide Class.

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

19 192. The ECPA confers a civil cause of action on “any person whose wire, oral, or
20 electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter.”
21 18 U.S.C. § 2520(a).

22 193. The ECPA protects both the sending and receipt of communications.

23 194. A violation of the ECPA occurs where any person “intentionally intercepts, endeavors
24 to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic
25 communication” or “intentionally discloses, or endeavors to disclose, to any other person the contents
26 of any . . . electronic communication, knowing or having reason to know that the information was
27 obtained through the [unlawful] interception of a[n] . . . electronic communication” or “intentionally
28 uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having

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

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

7 196. “Intercept” means “the aural or other acquisition of the contents of any wire,
8 electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18
9 U.S.C. § 2510(4).

10 197. “Electronic communication” means “any transfer of signs, signals, writing, images,
11 sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,
12 electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.”
13 18 U.S.C. § 2510(12).

14 198. “Contents” includes “any information concerning the substance, purport, or meaning”
15 of the communication at issue. 18 U.S.C. § 2510(8).

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

18 200. Plaintiff and Nationwide Class Members’ communications with Kaiser Permanente
19 through the Site, including the Portal, are electronic communications under the ECPA.

20 201. Whenever Plaintiff and Nationwide Class Members communicated with Kaiser
21 Permanente and/or their health care providers on the Site, Third Party Wiretappers, through the source
22 code Kaiser Permanente embedded and ran on its website, contemporaneously and intentionally
23 intercepted, and endeavored to intercept Plaintiff’s and Nationwide Class Members’ electronic
24 communications without authorization or consent.

25 202. Whenever Plaintiff and Nationwide Class Members communicated with Kaiser
26 Permanente and/or their health care providers on the Site, Kaiser Permanente, through the source
27 code it imbedded and ran on its website, contemporaneously and intentionally disclosed, and
28

1 endeavored to disclose the contents of Plaintiff's and Nationwide Class Members' electronic
2 communications to the Third Party Wiretappers, without authorization or consent, and knowing or
3 having reason to know that the electronic communications were obtained in violation of the ECPA.

4 203. Whenever Plaintiff and Nationwide Class Members communicated with Kaiser
5 Permanente and/or their health care providers on the Site, Kaiser Permanente, through the source
6 code it embedded and ran on the Site, contemporaneously and intentionally used, and endeavored to
7 use and allow the contents of Plaintiff's and Nationwide Class Members' electronic communications
8 to be disclosed and used for purposes other than providing health care services to Plaintiff and
9 Nationwide Class Members without authorization or consent, and knowing or having reason to know
10 that the electronic communications were obtained in violation of the ECPA.

11 204. Whenever Plaintiff and Nationwide Class Members communicated with Kaiser
12 Permanente and/or their health care providers on the Site, Kaiser Permanente, through the source
13 code it embedded and ran on the Site, contemporaneously and intentionally redirected the contents
14 of Plaintiff's and Nationwide Class Members' electronic communications while those
15 communications were in transmission, to persons or entities other than an addressee or intended
16 recipient of such communication, namely the Third Party Wiretappers.

17 205. Whenever Plaintiff and Nationwide Class Members communicated with Kaiser
18 Permanente and/or their health care providers on the Site, Kaiser Permanente, through the source
19 code it embedded and ran on the Site, contemporaneously and intentionally divulged the contents of
20 Plaintiff's and Nationwide Class Members' electronic communications while those communications
21 were in transmission, to persons or entities other than an addressee or intended recipient of such
22 communication, namely the Third Party Wiretappers.

23 206. The Third Party Wiretappers intentionally intercepted and used the contents of
24 Plaintiff's and Nationwide Class Members' electronic communications for the unauthorized purpose
25 of profiting from Plaintiff's and Nationwide Class Members' communications, including by
26 generating advertising revenue.

27
28

1 such devices and techniques has created a serious threat to the free exercise of personal liberties and
2 cannot be tolerated in a free and civilized society.” *Id.* § 630. CIPA is intended “to protect the right
3 of privacy of the people of this state.” *Id.*

4 215. To establish liability under section 631(a), Plaintiff need only establish that a
5 Defendant, “by means of any machine, instrument, or contrivance, or in any other manner,” did any
6 of the following:

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

11 Or

12 [ii] [W]illfully and without the consent of all parties to the communication, or in
13 any unauthorized manner, reads or attempts to read or learn the contents or meaning
14 of any message, report, or communication while the same is in transit or passing
15 over any wire, line or cable or is being sent from or received at any place within
16 this state,

17 Or

18 [iii] [U]ses, or attempts to use, in any manner, or for any purpose, or to
19 communicate in any way, any information so obtained,

20 Or

21 [iv] [A]ids, agrees with, employs, or conspires with any person or persons to
22 unlawfully do, or permit, or cause to be done any of the acts or things mentioned
23 above in this section.

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

26 217. Kaiser Permanente and the Third Party Wiretappers are each a “person” for the
27 purposes of CIPA.

28 218. Defendants maintain their headquarters in California, where they designed, contrived,
agreed, conspired, effectuated, aided, and/or received the interception and use of the contents of
Plaintiff and Class Members’ communications.

219. The Third Party Wiretappers’ code, Quantum Metric’s recording code, Plaintiff’s and
Class Members’ browsers and Plaintiff’s 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.

1 228. Plaintiff brings this claim individually and on behalf of the Nationwide Class, or
2 alternatively, on behalf of the California Sub-Class.

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

6 230. Kaiser Permanente intentionally intruded upon Plaintiff and Class Members' solitude
7 or seclusion when it disclosed communications it received from Plaintiff and Class Members, which
8 was intended to stay private, to Third Party Wiretappers.

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

16 232. Plaintiff and Class Members had a reasonable expectation of privacy over their
17 communications with Kaiser Permanente, including information obtained from their use of Kaiser
18 Permanente's Site, including the Portal.

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

23 234. The disclosure and collection of communications with Kaiser Permanente, including
24 information obtained from their use of Kaiser Permanente's Site through deceit is highly offensive to
25 a reasonable person. Plaintiff and Class Members reasonably expected that their communications
26 with Kaiser Permanente, including information obtained from their use of Kaiser Permanente's Site
27 would not be disclosed to third parties.

28

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

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

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

18 248. Defendants' conduct constituted a serious invasion of privacy that would be highly
19 offensive to a reasonable person in that: (i) the information disclosed by Kaiser Permanente and
20 collected by Third Party Wiretappers was highly sensitive and personal, as protected by the California
21 Constitution; (ii) Kaiser Permanente did not have authorization or consent to disclose this information
22 to any third party, including Third Party Wiretappers, and the Third Party Wiretappers did not have
23 authorization to collect this information; and (iii) the invasion deprived Plaintiff and Class Members
24 the ability to control the circulation of said information, which is considered a fundamental right to
25 privacy.

26
27
28

1 249. Defendants’ invasion violated the privacy rights of thousands of Class Members,
2 including Plaintiff, without authorization or consent. Their conduct constitutes a severe and egregious
3 breach of social norms.

4 250. As a direct and proximate result of Defendants’ actions, Plaintiff and Class Members
5 have had their privacy invaded and sustained damages and will continue to suffer damages.

6 251. Plaintiff and Class Members seek appropriate relief for that injury, including but not
7 limited to injunctive relief and damages that will reasonably compensate Plaintiff and Class Members
8 for the harm to their privacy interests as well as a disgorgement of profits earned as a result of their
9 intrusions upon Plaintiff’s and Class Members’ privacy.

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

11 **FIFTH CAUSE OF ACTION**
12 **Breach of Express Contract**
13 **(On Behalf of the Nationwide Breach of Contract Sub-Class or alternatively, On Behalf of the**
14 **California Breach of Contract Sub-Class)**

15 253. Plaintiff repeats and incorporates all other paragraphs as if fully set forth herein.

16 254. Plaintiff brings this claim individually and on behalf of the Nationwide Breach of
17 Contract Class, or alternatively, on behalf of the California Breach of Contract Sub-Class.

18 255. There exists an express contract between Plaintiff and Breach of Contract Class
19 Members on the one side, and Kaiser Permanente on the other, when Plaintiff and Breach of Contract
20 Class Members accessed information on the Kaiser Permanente Portal, namely the Terms and
21 Conditions and Privacy Policy for the Kaiser Permanente website (hereinafter referred to as the
22 “express contract” or “Site Terms and Conditions”). A true and correct copy of the Site Terms and
23 Conditions³⁶ currently in effect is attached hereto as Exhibit 1, and a copy of the Privacy Statement,
24 incorporated into the Terms and Conditions, is attached as Exhibit 2.

25 256. Specifically, at the bottom of the Portal Login Page, Kaiser Permanente agrees,
26 contracts, and warrants that: “By signing in, you agree to our website Terms & Conditions and
27 Privacy Statement.” <https://healthy.kaiserpermanente.org/southern-california/register> (last visited
28 May 3, 2023).

³⁶ The Terms and Conditions are materially identical for all Kaiser Permanente Regions.

1 257. The Kaiser Permanente Terms & Conditions, available via hyperlink, provides: “Any
2 personal information you submit to the Site (for yourself or someone else) is governed by our Website
3 and KP Mobile Application Privacy Statement.” *Terms & Conditions for our Website and Mobile*
4 *Application, supra* note 3.

5 258. In the Kaiser Permanente Privacy Statement, also available via hyperlink, Kaiser
6 Permanente also agrees, contracts, and warrants that Kaiser Permanente’s data collection “is collected
7 on an aggregate basis, which means that no personally identifiable information is associated with the
8 data.”

9 259. In the Kaiser Permanente Privacy Statement, Kaiser Permanente states that Kaiser
10 Permanente and its service providers may place “cookies” or similar technologies on the computer
11 hard drives of visitors to the Site, and further agrees, contracts, and warrants that information obtained
12 from cookies is only used to help Kaiser Permanente “tailor our Site to be more helpful and efficient
13 for our visitors.”

14 260. In the Kaiser Permanente Privacy Statement, Kaiser Permanente agrees, contracts, and
15 warrants that “[t]he cookie consists of a unique identifier that does not contain information about your
16 health history.”

17 261. The Kaiser Permanente Privacy Statement also states that Kaiser “may also
18 occasionally use ‘Web beacons’ (also known as ‘clear gifs,’ ‘Web bugs,’ ‘1-pixel gifs,’ etc.)” and
19 Kaiser Permanente also agrees, contracts, and warrants that Kaiser Permanente Kaiser will “not
20 collect any personal health information” through this technology.

21 262. Kaiser Permanente then makes the following promises in the Privacy Statement,
22 which is incorporated as part of the express contract:

- 23 • “Use and disclosure of health information includes using the information to provide
24 treatment to the individual, to make payments for such treatment, and to conduct
25 ongoing quality improvement activities. Our use and disclosure of an individual’s
personal information (including health information) is limited as required by state
and federal law.”
- 26 • “In addition to web logs, described below, Kaiser Permanente routinely gathers
27 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***
28 ***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

1 and overall usage. The information is not shared with other organizations for their
2 independent use.” (emphasis added).

3 263. In addition, Kaiser promises that “we do not collect any personally identifiable
4 information about visitors to the Site. The policies, sources, uses and disclosures of information are
5 outlined in Sections 1 through 20 that follow.”

6 264. Sections 2, 3, and 4 address “Web logs,” “Internet cookies,” and “Web Beacons,”
7 however, neither section describes the extensive information collection to which patient information
8 is subjected by the Kaiser website.

9 265. The Kaiser Permanente Privacy Statement does not disclose to Kaiser Plan Members
10 that Kaiser Permanente has aided, agreed with, employed, and/or conspired with third parties that are
11 recording all of the information that Kaiser Plan Members’ are sending, accessing, reviewing, or
12 receiving through the Site.

13 266. These terms create a contractual relationship between Kaiser Permanente and any
14 patient to whom it gives access to the Portal, including Plaintiff and Breach of Contract Class
15 Members.

16 267. Despite its assurances of privacy and confidentiality, Kaiser Permanente intentionally
17 incorporated the Third Party Wiretappers’ code and recording technology on the Kaiser Permanente
18 Site, including the Portal, disclosing the contents of Plaintiff and Breach of Contract Class Members’
19 information and confidential communications with Kaiser Permanente and its providers to Third
20 Party Wiretappers, including for advertising purposes.

21 268. In exchange for Kaiser Permanente’s provision of a secure website and patient Portal,
22 Plaintiff and Breach of Contract Class Members were able to make appointments, view medical
23 history, get test results, and find and communicate with doctors, among other things, by way of the
24 patient Portal, instead of doing so by other means, such as by phone or in person.

25 **Consent**

26 269. Kaiser Permanente requires Kaiser Plan Members to consent to the Site Terms and
27 Conditions in the process of signing up for, and using, the patient Portal.
28

Performance

274. Plaintiff John Doe and Breach of Contract Class Members performed under the express contract.

Kaiser Permanente’s Breach of the Express Contract

275. Kaiser Permanente materially breached its express contract with Plaintiff and Breach of Contract Class Members by disclosing to the Third Party Wiretappers, Plaintiff’s and Breach of Contract Class Members’ patient status, personally identifiable data, and confidential communications with Kaiser Permanente, thereby failing to provide Plaintiff and Breach of Contract Class Members with the secure method of communication it agreed to provide.

276. The patient health information Kaiser Permanente used and disclosed to unauthorized third parties includes:

- a. Breach of Contract 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 Class Members’ registration for the Portal;
- c. the date and time of every Breach of Contract Class Members’ sign-in and logoff of the “secure” the Portal;
- d. the contents of communications Breach of Contract Class Members’ exchange inside the “secure” Portal;
- e. the contents of communications Breach of Contract Class Members’ exchange after they have logged off the Portal;
- f. the contents of communications Breach of Contract Class Members’ exchange with Kaiser Permanente seeking providers who accept specific insurance products while still signed in to the “secure” Portal; and
- g. all other HTTPS communications patients exchange with Kaiser Permanente and its providers on the Site that Kaiser Permanente has permitted the third parties to correlate with the patient’s status as a patient, and the particular dates and times

1 for which they access the “secure” Portal.

2 277. The patient data Kaiser Permanente discloses (Plaintiff’s and Breach of Contract Class
3 Members’ patient status, personally identifiable data, and confidential communications with Kaiser
4 Permanente and its providers) is not aggregated as specified in the Privacy Statement.

5 278. Nevertheless, information that Plaintiff and Breach of Contract Class Members
6 reasonably thought was being transmitted “securely” to Kaiser Permanente was being disclosed by
7 Kaiser Permanente to unauthorized third parties as follows:

- 8 a. A Kaiser Plan Member signs in to the “secure” patient Portal;
- 9 b. On sign-in, Kaiser Permanente discloses the fact of the sign in to Adobe, Bing,
10 Google, Quantum Metric, and Twitter;
- 11 c. Once signed-in, if a Kaiser Plan Member clicked to, for example:
- 12 i. view tests, a disclosure of that action was made to Adobe, Bing, Google,
13 Quantum Metric, and Twitter of the specific tests; or,
- 14 ii. Find-A-Doctor, or set an appointment, a disclosure of that action was made
15 to Adobe, Bing, Google, Quantum Metric, and Twitter.
- 16 d. The above examples of patient communications about the doctor or the
17 appointment was shared with Adobe, Bing, Google, Quantum Metric, and Twitter
18 while the Kaiser Plan Member was still logged-in to the “secure” patient Portal;
19 and
- 20 e. On logoff, Kaiser Permanente discloses this action to Adobe, Bing, Google,
21 Quantum Metric, and Twitter.

22 279. Kaiser Permanente has failed to cure these breaches and continues to disclose to Third
23 Party Wiretappers, Plaintiff’s and Breach of Contract Class Members’ personally identifiable data
24 and communications with Kaiser Permanente.

25 **Plaintiff and Breach of Contract Class Members Were Damaged**

26 280. Defendants’ breach caused Plaintiff and Breach of Contract Class Members the
27 following damages, among others:

- 28 a. Nominal damages for each breach of contract by Defendants;

1 communications with Kaiser Permanente inside the Portal confidential when Plaintiff and Breach of
2 Contract Class Members used Kaiser Permanente’s patient Portal.

3 **Consideration**

4 287. The patient Portal is not a service Kaiser Permanente provides without receiving
5 anything from Plaintiff and other patients in return. To the contrary, Plaintiff’s and Breach of Contract
6 Class Members’ use of the Portal confers significant benefit upon Kaiser Permanente—a benefit to
7 which Kaiser Permanente is not entitled—including, but not limited to, increased efficiency,
8 optimized workflow, cost reduction, and receipt of incentive payments from the federal government
9 (United States Department of Health and Human Services) via the Meaningful Use Program.

10 288. As just one example, patients’ use of the patient Portal to access test results and make
11 appointments results in Kaiser Permanente being freed up from performing such tasks of scheduling
12 and reporting on test results for patients, thereby cutting down on long phone calls or in-office
13 communications, increasing efficiency and decreasing costs.

14 289. As a result, and as further noted above, Kaiser Permanente is able to more efficiently
15 allocate resources and benefits from improved—and, thus, less costly—patient outcomes and
16 increased patient loyalty.

17 **Performance**

18 290. Plaintiff John Doe and Breach of Contract -Class Members performed under the
19 implied contract.

20 **Kaiser Permanente’s Breach of the Implied Contract**

21 291. Kaiser Permanente materially breached its implied contract with Plaintiff and Breach
22 of Contract Class Members, by disclosing to third-party companies, Plaintiff and Breach of Contract
23 Class Members’ patient status, personally identifiable data, and confidential communications with
24 Kaiser Permanente made within the patient Portal, thereby failing to provide Plaintiff and Class
25 Members with the secure site it agreed to provide.

26 292. The patient health information Kaiser Permanente used and disclosed to unauthorized
27 third parties for marketing includes:

- 28 a. Breach of Contract Class Members’ IP addresses, User-Agent data, persistent cookie

1 identifiers, device identifiers, and/or browser fingerprint information—all of which
2 constitute personally identifiable data both alone and in combination with other data;

- 3 b. the date and time of Breach of Contract Class Members’ registration for the Portal;
4 c. the date and time of every Breach of Contract Class Member’s sign-in and logoff of
5 the “secure” Portal;
6 d. the contents of communications Breach of Contract Class Members exchange inside
7 the “secure” Portal;
8 e. the contents of communications Breach of Contract Class Members exchange after
9 they have logged off the Portal;
10 f. the contents of communications Breach of Contract Class Members exchange with
11 Kaiser Permanente seeking providers who accept specific insurance products while
12 still signed in to the “secure” Portal; and
13 g. all other HTTPS communications patients exchange with Kaiser Permanente at the
14 Site that Kaiser Permanente has permitted the third parties to correlate with the
15 Breach of Contract Class Members’ status as a patient and the particular dates and
16 times for which they access the “secure” Portal

17 293. The patient data Kaiser Permanente discloses (Plaintiff and Breach of Contract Class
18 Members patient status, personally identifiable data, and confidential communications with Kaiser
19 Permanente and its providers) is not aggregated as specified in the Privacy Statement.

20 294. Nevertheless, information that Plaintiff and Breach of Contract Class Members
21 reasonably thought was being transmitted “securely” to Kaiser Permanente within the patient Portal
22 was being disclosed by Kaiser Permanente to unauthorized third parties as follows:

- 23 a. A patient signs in to the “secure” patient Portal;
24 b. On sign-in, Kaiser Permanente discloses the fact of the sign in to Adobe, Bing,
25 Google, Quantum Metric, and Twitter;
26 c. Once signed-in, if a patient clicked to, for example:
27 d. view tests, a disclosure of that action was made to Adobe, Bing, Google, Quantum
28

1 Metric, and Twitter of the specific tests; or,

- 2 e. Find-A-Doctor, or set an appointment, a disclosure of that action was made to Adobe,
3 Bing, Google, Quantum Metric, and Twitter.
- 4 f. The above examples of patient communications about the doctor or the appointment
5 was shared with Adobe, Bing, Google, Quantum Metric, and Twitter while the
6 patient was still logged-in to the “secure” patient Portal; and
- 7 g. On logoff, Kaiser Permanente discloses this action to Adobe, Bing, Google,
8 Quantum Metric, and Twitter.

9 295. Kaiser Permanente has failed and refused to cure these breaches and continues to
10 disclose to unauthorized third parties, Plaintiff and Breach of Contract Class Members’ patient status,
11 personally identifiable data, and communications with Kaiser Permanente and its providers
12 exchanged on the Site, including the Portal.

13 **Plaintiff and Breach of Contract Class Members Were Damaged**

14 296. Defendants’ breach caused Plaintiff and Breach of Contract Class Members the
15 following damages, among others:

- 16 a. Nominal damages for each breach of contract by Defendants;
- 17 b. General damages for invasion of their rights in an amount to be determined by a
18 jury without reference to specific pecuniary harm;
- 19 c. Sensitive and confidential information that Plaintiff and Breach of Contract Class
20 Members intended to remain private is no longer private;
- 21 d. Defendants eroded the essential confidential nature of the provider-patient
22 relationship;
- 23 e. Defendants took something of value from Plaintiff and Breach of Contract Class
24 Members and derived benefit therefrom without Plaintiff’s and Breach of
25 Contract Class Members’ knowledge or informed consent and without sharing
26 the benefit of such value;
- 27 f. Plaintiff and Breach of Contract Class Members did not get the full value of the
28 medical services for which they paid, which included Defendants’ duty to

1 maintain confidentiality;

2 g. Defendants' actions diminished the value of Plaintiff and Breach of Contract
3 Class Members' personal information;

4 h. Defendants' actions violated the property rights Plaintiff and Breach of Contract
5 Class Members enjoy in their private communications; and

6 i. Defendants' actions violated the property rights Plaintiff and Breach of Contract
7 Class Members enjoy in their personally identifiable medical data and
8 communication.

9 297. Plaintiff and Breach of Contract Class Members also seek attorney's fee and costs on
10 this claim to the extent allowable.

11 **VIII. PRAYER FOR RELIEF**

12 WHEREFORE, Plaintiff, individually and on behalf of the proposed Classes, respectfully
13 requests that the Court enter an order:

14 A. Certifying this case as a class action on behalf of the Classes defined above, appointing
15 Plaintiff as the representative of the Classes, and appointing Plaintiff's counsel as the
16 Class Counsel for the Classes;

17 B. Declaring that Defendants' conduct, as set forth above, violates the laws cited herein;

18 C. Awarding damages, including nominal, statutory, and punitive damages where
19 applicable, to Plaintiff and the Classes in an amount to be determined at trial;

20 D. Awarding Plaintiff and the Classes their reasonable litigation expenses, costs and
21 attorneys' fees;

22 E. Awarding Plaintiff and the Classes pre- and post-judgment interest, to the extent
23 allowable;

24 F. Awarding such other further injunctive and declaratory relief as is necessary to protect
25 the interests of Plaintiff and the Classes; and

26 G. Awarding such other and further relief as the Court deems reasonable and just.
27
28

1 **IX. DEMAND FOR JURY TRIAL**

2 Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff demands a jury trial
3 as to all issues triable by a jury.

4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DATED: May 5, 2023

Respectfully submitted,

**KESSLER TOPAZ
MELTZER & CHECK, LLP**

/s/ Jennifer L. Joost
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
jmeltzer@ktmc.com
Melissa L. Yeates
myeates@ktmc.com
Tyler S. Graden
tgraden@ktmc.com
Jordan E. Jacobson
jjacobson@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056

Counsel for Plaintiff and the proposed Classes

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Kaiser Permanente Shares Website Visitors' Info with Third Parties, Class Action Says](#)
