Robert Mackey (SBN 125961)
bobmackeyesq@aol.com
LAW OFFICES OF ROBERT MACKEY
660 Baker Street
Building A, Ste. 201
Costa Mesa, CA 92626
Tel: (412) 370-9110
Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ALEXIS SUTTER, on behalf of herself and all others similarly situated Plaintiff, vs. KAISER FOUNDATION HEALTH PLAN, INC. Defendant.	CASE NO.: **CLASS ACTION COMPLAINT** (1) Violation Of the Electronic Communications Privacy Act; (2) Breach of Express Contract (3) Breach Of Implied Duty of Good Faith And Fair Dealing (4) Breach of Implied Contract (5) Negligence (6) Breach of Fiduciary Duty (7) Unjust Enrichment **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Alexis Sutter ("**Plaintiff**"), individually and on behalf of all others similarly situated, bring this class action lawsuit against Kaiser Foundation Health Plan, Inc. ("**Kaiser**"). Plaintiff's allegations are based upon personal knowledge as to herself and her own acts, and upon information and good faith belief as to all other matters based on the investigation conducted by undersigned counsel.

INTRODUCTION

1. This case seeks legal redress for Defendant's conscious decision to install tracking technologies on its website and mobile applications to collect its patients' personal health

information and disclose that highly sensitive information to third party platforms like Microsoft, Facebook and Google without consent.

2. Defendant is a not-for-profit healthcare organization associated with the Kaiser Permanente brand. Defendant oversees one of the largest managed care consortiums in the United States.

3. In order to market, sell and provide its healthcare offerings, Defendant owns, maintains and operates a website and mobile applications ("Website and Apps").

4. As detailed herein, Defendant disregarded the privacy rights of its patients who used its Website and Apps ("**Users**" or "**Class Members**") by installing, configuring and using tracking technologies on its Website and Apps to collect and divulge their personally identifiable information ("**PII**") and protected health information ("**PHI**" and collectively, "**Private Information**") to Meta Platform Inc. d/b/a Facebook and other technology companies.[1]

5. Unbeknownst to Users and without their authorization or informed consent, Defendant installed invisible third-party tracking technology on its Website and Apps in order to intercept Users' PII and PHI with the express purpose of disclosing that Private Information to third parties such as Meta and/or Google LLC in violation of HIPAA Privacy Rule and 42 U.S.C. § 1320d-6 as well as state, federal and common law.

6. Meta and other companies then access and use the Private Information by associating it with the individual User.

7. As an example of how one of these insidious tracking technologies used by Defendant functions, consider the Pixel.

8. Meta offers a tool called the Meta Pixel that associates individual browsing data that User's personal Facebook account. Meta is able to personally identify each User with an active Facebook account by using the "c_user" cookie that Meta stores in users' browsers and which

[1] *See* Alicia Hope, *Healthcare Provider Kaiser Permanente Discloses Online Tracking Data Breach Impacting 13.4 Million, cpomagazine.com* (May 3, 2023) *available at* https://www.cpomagazine.com/cyber-security/healthcare-provider-kaiser-permanente-discloses-online-tracking-data-breach-impacting-13-4-million/ (last visited May 10, 2024).

reveals a Facebook account-holder's unique "FID" value. Defendant does not provide many details but notes that other tracking technologies are used as well, presumably with the same functionality across different User profiles and accounts.

9. With the Meta Pixel, a user's FID is linked to their Facebook profile which personally identifies the user through a wide range of demographic and other information about the user including the User's name, pictures, personal interests, work history, relationship status and other details. Because the user's FID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the FID to quickly and easily locate, access, and view the user's corresponding Facebook profile.[2]

10. Notably, the Pixel collects data regardless of whether the User has a Facebook account as Facebook maintains "shadow profiles" on users without Facebook accounts and links the information collected via the Pixel to the user's real-world identity using their shadow profile.[3]

11. The Pixel intercepts and discloses the information of every Facebook user that visits the Defendant's Website and Apps in the same way.

12. Defendant has admitted that numerous interactions with the Website and Apps were leaked, including patient names and IP addresses, whether they were signed into Kaiser accounts, how they interacted with the Website and Apps, and the search terms they entered into the organization's encyclopedia of health terms.[4]

13. Plaintiff and Class Members who visited and used Defendant's Website and Apps thought they were communicating with only their trusted healthcare providers, and reasonably believed that their sensitive and private PHI would be guarded with the utmost care. In browsing

---

[2] To find the Facebook account associated with a particular c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

[3] *See* Russell Brandom, *Shadow Profiles Are The Biggest Flaw In Facebook's Privacy Defense*, TheVerge.com (Apr 11, 2018), *available at* https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (last visited May 10, 2024).

[4] *See* Troy Wolverton, *Here's what you should know about the Kaiser Permanente data leak*, sfexaminer.com (May 7, 2024) *available at* https://www.sfexaminer.com/news/technology/what-you-should-know-about-the-kaiser-permanente-data-leak/article_7d6f9256-0be7-11ef-a085-533bb1c22009.html (last visited May 10, 2024).

Defendant's Website and Apps—be it to make an appointment, locate a doctor with a specific specialty, find sensitive information about their diagnosis, or investigate treatment for their diagnosis—Plaintiff and Class Members did not expect that every search (including exact words and phrases they typed into Defendant's Website and Apps search bars), extremely sensitive PHI such as health conditions (e.g., breast cancer or pregnancy), diagnoses (e.g., stroke, arthritis, or AIDS), procedures sought, treatment status, and/or their treating physician, would be intercepted, captured and otherwise shared with Facebook and other technology companies in order to target Plaintiff and Class Members with ads, in conscious disregard of their privacy rights.

14. Plaintiff continued to have her privacy violated when her Private Information was used to turn a profit by way of targeted advertising related to her respective medical conditions and treatments sought.

15. Defendant knew that by embedding tracking technologies on its Website and Apps it was permitting Facebook, Google, X (formerly Twitter), Microsoft, and various other companies to collect and use Plaintiff's and Class Members' Private Information, including sensitive medical information.

16. Defendant (or any third parties) did not obtain Plaintiff's and Class Members' prior consent before sharing their sensitive, confidential communications with third parties such as Facebook.

17. Defendant's actions constitute an extreme invasion of Plaintiff's and Class Members' right to privacy and violate federal and state statutory and common law as well as Defendant's own Privacy Policies that affirmatively and unequivocally state that any personal information provided to Defendant will remain secure and protected.

18. The privacy policy posted by Defendant states that "This Privacy Statement applies to the Websites, which are owned and operated by Kaiser Foundation Health Plan, Inc. ("Kaiser Permanente", "KP"). This Privacy Statement describes how Kaiser Permanente collects and uses

information that is collected from your use of the Website."[5]

19. The privacy statement goes on to say "[w]e do not sell or rent personal information about visitors to the Websites."[6]

20. The privacy statement describes a number of uses of user data before explicitly claiming that "[t]he data is collected on an aggregate basis, which means that no personally identifiable information is associated with the data. This data helps us improve our content and overall usage. **The information is not shared with other organizations for their independent use.**"[7]

21. As a result of Defendant's conduct, Plaintiff and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lack of trust in communicating with doctors online; (iii) emotional distress and heightened concerns related to the release of Private Information to third parties; (iv) loss of the benefit of the bargain; (v) diminution of value of the Private Information; (vi) statutory damages and (vii) continued and ongoing risk to their Private Information.

22. Plaintiff and Class Members have a substantial risk of future harm, and thus injury in fact, due to the continued and ongoing risk of misuse of their Private Information that was shared by Defendant with unauthorized third parties.

23. Plaintiff seek, on behalf of herself and a class of similarly situated persons, to remedy these harms and therefore assert the following statutory and common law claims against Defendant: (i) Violation of Electronic Communications Privacy Act, 18 U.S.C. §2511(1), *et seq*; (ii) Negligence; (iii) Breach of Express Contract, (iv) Breach of Implied Duty of Good Faith and Fair Dealing, (v) Breach of Implied Contract, (vi) Breach of Fiduciary Duty and (vii) Unjust Enrichment.

PARTIES

[5] *Privacy statement for our website* (Jan. 20, 2021), https://healthinnovation.kp.org/privacy-policy/

[6] *Id.*

[7] *Id*. (emphasis added)

24. Plaintiff Alexis Sutter is a Virginia citizen, where she intends to remain indefinitely.

25. Defendant Kaiser Foundation Health Plan, Inc. is a healthcare consortium. Defendant is incorporated in California with its principal place of business located at One Kaiser Plaza Oakland, CA 94612.

JURISDICTION & VENUE

26. This Court has jurisdiction over the subject matter of the action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than one hundred (100) putative class members defined below, and minimal diversity exists because a significant portion of putative class members are citizens of a state different from the citizenship of at least one Defendant.

27. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District. Defendant received substantial compensation from offering healthcare services in this District, and Defendant made numerous misrepresentations which had a substantial effect in this District, including, but not limited to, representing that Defendant will only disclose Private Information provided to them under certain circumstances, ***which do not*** include disclosure of Private Information for marketing purposes.

28. Defendant is subject to personal jurisdiction in California because Defendant maintains its principal place of business in California and is authorized to conduct and is conducting business in California.

PLAINTIFF'S EXPERIENCE

29. Plaintiff Alexis Sutter is a resident of Annandale, Virginia.

30. Plaintiff has been a patient of Defendant's since January of 2022, and prior to that from 2007 through 2012.

31. During the relevant time period (when the Defendant's tracking technologies were present) Plaintiff used Defendant's Website and Apps to schedule appointments and browse information about Defendant's services and offerings.

32. On May 8, 2024, Plaintiff received a cryptic, templated email from Defendant notifying her that her PHI and PII had been compromised by Defendant's use of tracking technologies.

33. Defendant's letter failed to inform Plaintiff of exactly what PHI and PII had been compromised, and with which parties it had been shared.

34. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to third parties can only be determined through formal discovery.

35. Plaintiff reasonably expected that her communications with Defendant via the Website and Apps were confidential, solely between herself and Defendants, and that such communications would not be transmitted to or intercepted by a third party.

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

37. By failing to do so, Defendant breached Plaintiff's privacy and unlawfully disclosed her Private Information.

38. Prior to the email of May 8, 2024, Defendant did not inform Plaintiff that it had shared her Private Information with third parties.

39. Plaintiff would not have utilized Defendant's medical services and/or used its Website and Apps or would have paid much less for Defendant's services had she known that her Private Information would be captured and disclosed to third parties like Facebook without her consent.

FACTUAL BACKGROUND

A. The Irresponsible Use of Invisible Tracking Codes by Healthcare Providers to Send Meta People's Data for its Advertising Business.

40. Again taking Meta as just one example of how these tracking tools work, one begins to understand the depth and breadth of PHI and PII that is shared with third parties.

41. Meta operates the world's largest social media company whose revenue is derived almost entirely from selling targeted advertising.

42. The Meta Pixel and other third-party tracking tools also collect and transmit information from Defendant that identifies a Facebook user's status as a patient and other health information that is protected by federal and state law. This occurs through tools and tactics that Facebook encourages its healthcare Partners to use, including uploading patient lists to Facebook for use in its advertising systems.

43. Meta associates the information it obtains via the Meta Pixel with other information regarding the User, using personal identifiers that are transmitted concurrently with other information the Pixel is configured to collect.

44. For Facebook account holders, these identifiers include the "c_user" cookie IDs, which allow Meta to link data to a particular Facebook account. For both Facebook account holders and users who do not have a Facebook account, these identifiers also include cookies that Meta ties to their browser.

45. Realizing the value of having direct access to millions of consumers, in 2007, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming it to be a "completely new way of advertising online" that would allow "advertisers to deliver more tailored and relevant ads."[8]

46. One of its most powerful advertising tools is Meta Pixel, formerly known as Facebook Pixel, which launched in 2015.

47. Ad targeting has been extremely successful due, in large part, to Facebook's ability to target people at a granular level. "Among many possible target audiences, Facebook offers advertisers, [for example,] 1.5 million people 'whose activity on Facebook suggests that they're

[8] *Facebook Unveils Facebook Ads*, META (November 6, 2007), https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/.

more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'"[9]

48. The Meta Pixel is a free and publicly available "piece of code" that third-party web developers can install on their Website and Apps to "measure, optimize and build audiences for … ad campaigns."[10]

49. Meta describes the Pixel as "a snippet of JavaScript code" that "relies on Facebook cookies, which enable [Facebook] to match … Website and Apps visitors to their respective Facebook user accounts.[11]

50. Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel "can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart."[12]

51. Meta tells advertisers that the Meta Pixel will improve their Facebook advertising, including by allowing them to:

a. "optimize the delivery of your ads" and "[e]nsure your ads reach the people most likely to take action;" and

b. "create Custom Audiences from Website and Apps visitors" and create "[d]ynamic ads [to] help you automatically show Website and Apps visitors the products they viewed on your Website and Apps—or related ones."[13]

[9] Natasha Singer, *What You Don't Know about How Facebook Uses Your Data* (April 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.
[10] *Meta Pixel* (2023), https://www.facebook.com/business/tools/meta-pixel.
[11] *Meta Pixel* (2023), https://developers.facebook.com/docs/meta-pixel/.
[12] *Meta Pixel* (2023), https://www.facebook.com/business/tools/meta-pixel.
[13] *Id.*

52. Meta explains that the Pixel "log[s] when someone takes an action on your Website and Apps" such as "adding an item to their shopping cart or making a purchase," and the user's subsequent action:

> Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads.

53. The Meta Pixel is customizable and web developers can choose the actions the Pixel will track and measure on a particular webpage.

54. Meta advises web developers to place the Pixel early in the source code[14] for any given webpage or Website to ensure that visitors will be tracked before they leave the webpage or Website and Apps.[15]

55. Meta's "Health" division is dedicated to marketing to and servicing Meta's healthcare "Partners." Meta defines its "Partners" to include businesses that use Meta's products, including the Meta Pixel or Meta Audience Network tools to advertise, market, or support their products and services.

56. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted

[14] Source code is a collection of instructions (readable by humans) that programmers write using computer programming languages such as JavaScript, PHP, and Python. When the programmer writes a set or line of source code, it is implemented into an application, Website and Apps, or another computer program. Then, that code can provide instructions to the Website and Apps on how to function. *What is Source Code & Why Is It Important?* (July 19, 2023), https://blog.hubspot.com/Website and Apps/what-is-source-code (last visited Apr. 4, 2024).

[15] *Meta Pixel: Get Started* (2023), *https://developers.facebook.com/docs/meta- pixel/get-started.*

advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.

57. Healthcare providers like Defendant encourage Plaintiff and Class Members to access and use various digital tools via its Website and Apps to, among other things, receive healthcare services, in order to gain additional insights into its Users, improve its return on marketing dollars and, ultimately, increase its revenue.

58. In exchange for installing the Pixels, Facebook provided Defendant with analytics about the advertisements it has placed as well as tools to target people who have visited its Website and Apps.

59. Upon information and belief, Defendant and other companies utilized Plaintiff's and Class Members' sensitive information and data collected by the Meta Pixels on Defendant's Website and Apps in order to advertise to these individuals later on Meta's social platforms.

60. If a healthcare provider, such as Defendant, installs the Meta Pixel code as Meta recommends, patients' actions on the provider's Website and Apps are contemporaneously redirected to Meta.

61. For example, when a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Meta's source code commands the patient's computing device to send the content of the patient's communication to Meta while the patient is communicating with their healthcare provider.

62. In other words, by design, Meta receives the content of a patient's portal log in communication immediately when the patient clicks the log-in button—even before the healthcare provider receives it.

63. Thus, the Meta "pixel allows Facebook to be a silent third-party watching whatever you're doing,"[16] which in this case included the content of Defendant's patients' communications with its Website and Apps, including their PHI.

[16] Jefferson Graham, *Facebook spies on us but not by recording our calls. Here's how the social network knows everything* (Apr. 4, 2020),

64. For Facebook, the Pixel acts as a conduit of information, sending the information it collects to Facebook through scripts running in the User's internet browser, via data packets labeled with PII, including the User's IP address, the Facebook c_user cookie and third-party cookies allowing Facebook to link the data collected by Meta Pixel to the specific Facebook user.[17]

65. A recent investigation by The Markup revealed that the Meta Pixel was installed inside password-protected patient portals of at least seven U.S. health systems, giving Facebook access to even more patient communications with their providers.[18]

66. David Holtzman, a health privacy consultant was "deeply troubled" by the results of The Markup's investigation and indicated "it is quite likely a HIPAA violation" by the hospitals, such as Defendant.[19]

67. Facebook's access to use even only some of these data points—such as just a "descriptive" webpage URL—is problematic. As Laura Lazaro Cabrera, a legal officer at Privacy International, explained: "Think about what you can learn from a URL that says something about scheduling an abortion' . . . 'Facebook is in the business of developing algorithms. They know what sorts of information can act as a proxy for personal data."[20]

68. The collection and use of this data raises serious concerns about user privacy and the potential misuse of personal information. For example, when Users browse Defendant's Website and Apps, every step of their activity is tracked and monitored. By analyzing this data using algorithms and machine learning techniques, Facebook (and other entities tracking this

---

https://www.usatoday.com/story/tech/2020/03/04/facebook-not-recording-our-calls-but-has-other-ways-snoop/4795519002/.

[17] The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users. *See* Maciej Zawadziński & Michal Wlosik, *What Facebook's First-Party Cookie Means for AdTech* (June 8, 2022), https://clearcode.cc/blog/facebook-first-party-cookie-adtech/.

[18] *See* Feathers, *supra*, note 16.

[19] *Id.*

[20] Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, THE MARKUP (Sept. 25, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients.

information) can learn a chilling level of detail about Users' medical conditions, behavioral patterns, preferences, and interests.

69. This data can be used not only to provide personalized and targeted content and advertising, but also for more nefarious purposes, such as tracking and surveillance. Moreover, the misuse of this data could potentially lead to the spread of false or misleading information, which could have serious consequences, particularly in the case of health-related information.

70. As pointed out by the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS), impermissible disclosures of such data in the healthcare context "may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI…. this tracking information could also be misused to promote misinformation, identity theft, stalking, and harassment."[21]

71. Unfortunately, several recent reports detail the widespread use of third-party tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to surreptitiously capture and to disclose their Users' Private Information.[22] Estimates are that over 664 hospital systems and providers utilize some form of tracking technology on their digital properties.[23]

B. Defendant Disclosed Patient Healthcare Information, Including Patient Status, in Violation of the HIPAA Privacy Rule.

[21] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Mar. 12, 2024).

[22] The Markup reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment. Todd Feathers, *Facebook Is Receiving Sensitive Medical Information from Hospital Website and Appss*, *supra*, note 16.

[23] Dave Muoio & Annie Burky, *Advocate Aurora, WakeMed get served class action over Meta's alleged patient data mining*, FIERCE HEALTHCARE (November 4, 2022), https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-Website and Appss-collecting-patient-data-facebook.

72. Healthcare entities collecting and disclosing Users' Private Information face significant legal exposure under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which applies specifically to healthcare providers, health insurance providers and healthcare data clearinghouses.[24]

73. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information ("IIHI") that is held or transmitted.[25] This is information that can be used to identify, contact, or locate a single person or can be used with other sources to identify a single individual.

74. Plaintiff's IIHI captured by third party tracking almost certainly included their unique personal identifiers such as their Facebook ID, IP address, device identifiers and browser "fingerprints."

75. HIPAA also protects against revealing an individual's status as a patient of a healthcare provider.[26]

76. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1).

77. Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

78. Defendant unlawfully revealed Plaintiff's and Class Members' patient status to Facebook and likely other unauthorized third parties in violation of HIPAA when the Meta Pixel

---

[24] *Health Information Privacy* (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[25] The HIPAA Privacy Rule protects all electronically protected health information a covered entity like Defendant "created, received, maintained, or transmitted" in electronic form. *See* 45 C.F.R. § 160.103.

[26] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Apr. 4, 2024).

captured and disclosed Plaintiff's and Class Members' activity on patient-dedicated webpages of the Website and Apps, such as Patient Financial Services, Patient Education Resources, Schedule an Appointment, and the Patient Portal.

A. HIPAA's Protections Do Not Exclude Internet Marketing.

79. The Office for Civil Rights at HHS has made clear, in a recently updated bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[27]

80. Here, Defendant provided patient information to third parties in violation of the Privacy Rule. HHS has repeatedly instructed for years that patient status is protected by the HIPAA Privacy Rule:

> a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);
>
> b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002); and

[27] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (emphasis added) (updated March 18, 2024) (last visited April 4, 2024).

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

81. In addition, the Office for Civil Rights at HHS' Bulletin expressly provides that "**[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.**"[28]

82. Tracking technology vendors like Facebook and Google are considered business associates under HIPAA where, as here, they provide services to Defendant and receive and maintain PHI.

> Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (*e.g.* health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the Website and Apps of a covered health clinic for health services and that Website and Apps uses third party tracking technologies, then the Website and Apps might automatically transmit information regarding the appointment and

[28] *Id.*

> the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.[29]

83. The Bulletin further explained that health care providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address) even if no treatment information is included and even if the individual does not have a relationship with the health care provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> **Some regulated entities may be disclosing a variety of information to tracking technology vendors through tracking technologies placed on the regulated entity's Website and Apps or mobile app, such as information that the individual types or selects when they use regulated entities' Website and Appss or mobile apps**. The information disclosed might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, device IDs, or any unique identifying code.
>
> ---
>
> IIHI collected on a regulated entity's Website and Apps or mobile app generally is PHI, **even if the individual does not have an existing relationship with the regulated entity** and even if the IIHI, such as in some circumstances IP address or geographic

[29] *Id.*

> location, does not include specific treatment or billing information like dates and types of health care services.[30]

84. HIPAA applies to Defendant's webpages with tracking technologies even outside the patient portal:

Tracking on unauthenticated webpages

> Regulated entities may also have unauthenticated webpages, which are webpages that do not require users to log in before they are able to access the webpage, such as a webpage with general information about the regulated entity like their location, visiting hours, employment opportunities, or their policies and procedures… **in some cases, tracking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to the tracking technology vendors**. Regulated entities are required to "[e]nsure the confidentiality, integrity, and availability of all electronic PHI the [regulated entity] creates, receives, maintains, or transmits." Thus, regulated entities that are considering the use of online tracking technologies should consider whether any PHI will be transmitted to a tracking technology vendor, and take appropriate steps consistent with the HIPAA Rules.[31]

[30] *Id.* (emphasis added).
[31] *Id.* (emphasis added).

85. HHS explained that, if the online tracking technologies on the webpages have access to information that relates to an individual's past, present, or future health, health care, or payment for health care, that is a disclosure of PHI, for example:

> [I]f an individual were looking at a hospital's webpage **listing its oncology services** to seek a second opinion on treatment options for their brain tumor, **the collection and transmission of the individual's IP address, geographic location, or other identifying information showing their visit to that webpage is a disclosure of PHI** to the extent that the information is both identifiable and related to the individual's health or future health care.

86. HHS also explained in the Bulletin that tracking technologies on health care providers' patient portals "generally have access to PHI" and may access diagnoses and treatment information, in addition to other sensitive data:

> Tracking on user-authenticated webpages
>
> Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. **Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. Tracking technologies within user-authenticated webpages may even have access to an individual's

> diagnosis and treatment information, prescription information, billing information, or other information within the portal. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to only use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its Website and Apps is protected and secured in accordance with the HIPAA Security Rule.[32]

87. The Bulletin is not a pronouncement of new law, but instead a reminder to covered entities and business associates of their longstanding obligations under existing guidance.

88. The Bulletin notes that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," then explains how online tracking technologies violate the same HIPAA rules that have existed for decades.[33]

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

90. As a result, a healthcare provider like Defendant may not disclose PHI to a tracking technology vendor, like Meta, unless it has properly notified its Website and App Users and entered into a business associate agreement with the vendor in question.

---

[32] *Id.* (emphasis added).

[33] *Id.* (citing, *e.g.*, Modifications of the HIPAA [Rules], Final Rule," 78 FR 5566, 5598, a rulemaking notice from January 25, 2013, which stated: "[P]rotected health information … may not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a covered entity, then it is protected health information by definition since it is indicative that the individual received health care services or benefits from the covered entity, and therefore it must be protected … in accordance with the HIPAA rules." at n. 22).

B. Defendant Transmitted a Broad Spectrum of Plaintiff's & Class Members' Identifiable Health Information to Meta via the Meta Tracking Tools.

91. Every Website is comprised of "Markup" and "Source Code." Markup consists of the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Website.

92. Source Code is a set of instructions that commands the Website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code. Source Code is designed to be readable by humans and formatted in a way that developers and other users can understand.

93. In addition to controlling a Website's Markup, Source Code executes a host of other programmatic instructions including the ability to command a Website and Apps user's browser to send data transmissions to third parties like Facebook, via the Meta Pixel.[34]

94. Defendant's tracking technologies, embedded in its JavaScript Source Code on the Website and Apps, manipulated a User's browser by secretly instructing it to duplicate a User's communications (HTTP Requests) and sending those communications to third parties.

95. This occurs because these technologies are programmed to automatically track and transmit Users' communications, and this occurs contemporaneously, invisibly, and without the Users' knowledge.

96. The information Defendant sent to Meta from its use of the Meta Pixel and other tracking tools likely includes, but is not limited to, the following:

a. The exact search terms entered by a User on the Website and Apps, including searches for the User's medical symptoms and conditions, specific medical providers and their specialty, and treatments sought;

[34] These Pixels or web bugs are tiny image files that are invisible to Website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware of them.

b. descriptive URLs that describe the categories of the Website and Apps, categories that describe the current section of the Website and Apps, and the referrer URL that caused navigation to the current page;

c. the communications a User exchanges through Defendant's Website and Apps by clicking and viewing webpages, including communications about providers and specialists, conditions, and treatments, along with the timing of those communications, including, upon information and good faith belief, whether they are made while a User is still logged in to the Patient Portal or around the same time that the User has scheduled an appointment, called the medical provider, or logged in or out of the Patient Portal;

d. when a User sets up or schedules an appointment;

e. information that a User clicks on in an appointment form;

f. when a User clicks a button to call the provider from a mobile device directly from Defendant's Website and Apps;

g. when a User clicks to register for the Patient Portal, clicks to log into the Portal, and/or accesses other patient-dedicated web pages; and

h. the same or substantially similar communications that patients exchange with health insurance companies, pharmacies, and prescription drug companies.

97. Thus, Defendant is, in essence, handing patients a tapped device and once one of its webpages is loaded into the User's browser, the software-based wiretap is quietly waiting for private communications on the webpage to trigger the tap, which intercepts those communications—intended only for Defendant—and transmits those communications to unauthorized third parties such as Facebook.

98. Defendant's Source Code and underlying HTTP Requests and Responses were likely configured to share the patient's personal information with third parties, including the fact that a User was looking for doctors to assist with their heart disease, diabetes, or stroke diagnosis — along with the User's unique personal identifiers.

99. After announcing this data breach, and following a wave of negative press and litigation against other healthcare companies for the same unlawful activities, Defendant removed the Meta Pixel and other tracking technologies from its Website and Apps and has re-configured its source code.

100. Before these tracking tools were removed, Defendant was sharing inordinate amounts of Plaintiff's and Class Members' PII and PHI with third parties.

C. Plaintiff and Class Members Reasonably Believed That Their Confidential Medical Information Would Not Be Shared with Third Parties.

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

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

103. Personal data privacy and obtaining consent to share Private Information are material to Plaintiff and Class Members.

104. Plaintiff and Class Members relied to their detriment on Defendant's uniform representations and omissions regarding protection privacy, limited uses, and lack of sharing of their Private Information.

105. Now that their sensitive personal and medical information is in possession of third parties, Plaintiff and Class Members face a constant threat of continued harm including bombardment of targeted advertisements based on the unauthorized disclosure of their personal data. Collection and sharing of such sensitive information without consent or notice poses a great threat to individuals by subjecting them to the never-ending threat of identity theft, fraud, phishing scams, and harassment.

D. Plaintiff and Class Members Have No Way of Determining Widespread Usage of Invisible Tracking Tools.

106. Plaintiff and Class Members could not reasonable foresee that tracking tools were in use because they are invisibly embedded within Defendant's web pages that Users might interact with.[35] Patients and Users of Defendant's Website and Apps do not receive any alerts during their uses of Defendant's Website and Apps stating that Defendant tracks and shares sensitive medical data with Facebook, allowing Facebook and other third parties to subsequently target all Users of Defendant's Website and Apps for marketing purposes.

107. Plaintiff and Class Members trusted Defendant's Website and Apps when inputting sensitive and valuable Private Information. Had Defendant disclosed to Plaintiff and Class Members that every click, every search, and every input of sensitive information was being tracked, recorded, collected, and disclosed to third parties, Plaintiff and Class Members would not have trusted Defendant's Website and Apps to input such sensitive information.

108. Defendant knew or should have known that Plaintiff and Class Members would reasonably rely on and trust Defendant's promises regarding the tracking privacy and uses of their Private Information. Furthermore, any person visiting a health website or related applications has

[35] *See, e.g.*, FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FED. TRADE COMM'N (March 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.

a reasonable understanding that medical providers must adhere to strict confidentiality protocols and are bound not to share any medical information without their consent.

109. By collecting and sharing Users' Private Information with Facebook and other unauthorized third parties, Defendant caused harm to Plaintiff, Class Members, and all affected individuals.

110. Furthermore, once Private Information is shared with third parties, such information may not be effectively removed, even though it includes personal and private information.

111. Plaintiff fell victim to Defendant's unlawful collection and sharing of their sensitive medical information using the Meta Pixel tracking code on Defendant's Website and Apps.

E. Defendant Knew Plaintiff's Private Information Included Sensitive Medical Information, Including Medical Records.

112. By virtue of how the Meta Pixel and other tracking tools work, i.e., sending all interactions on a Website to a third party, Defendant was aware that its Users' Private Information would be sent to third parties when they researched specific medical conditions and/or treatments, looked up providers, made appointments, typed specific medical queries into the search bar, and otherwise interacted with Defendant's Website and Apps.

113. At all times relevant herein Meta notified its partners, including Defendant, to have the rights to collect, use, and share user data before providing any data to Meta.[36] Although Meta's

[36] *See In re Meta Pixel Healthcare Litig.*, No. 22-cv-03580-WHO, 2022 U.S. Dist. LEXIS 230754, at *13-14 (N.D. Cal. Dec. 22, 2022).

intent is questionable, Defendant had been on notice of this Pixel-tracking ever since they activated such Pixel technology on its Website and Apps.

114. Meta changed this provision again in July 2022, while still requiring partners to have the right to share patient information with Meta:[37]

> **Information from partners.**
> Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities off of our Products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services —whether or not you have an account or are logged into our Products. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.
>
> Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. Learn more about the types of partners we receive data from.
>
> To learn more about how we use cookies in connection with Meta Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.

How do we collect or receive this information from partners?

Partners use our Business Tools, integrations and Meta Audience Network technologies to share information with us.

These Partners collect your information when you visit their site or app or use their services, or through other businesses or organizations they work with. We require Partners to have the right to collect, use and share your information before giving it to us.

[37] Meta, *Data Policy: Information from Partners, vendors and third parties* (Jan. 1, 2023), https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors.

115. Defendant had the explicit option to disable the Pixel technology on its Website and Apps, but chose not to exercise this option, thereby continuing to share data with Facebook despite the availability of preventive measures.

116. Meta advised third party entities, like Defendant, to refrain from sending any information they did not have the legal right to send and expressly emphasized not to transmit health information. Yet, Defendant, in direct contravention of these disclosures, and more importantly despite Defendant's promises to keep all health-related data about patients confidential, continued to employ Pixel tracking on its Website and Apps, thereby sharing sensitive patient data without proper authorization or consent.

F. Plaintiff and Class Members Have a Reasonable Expectation of Privacy in Their Private Information, Especially with Respect to Sensitive Medical Information.

117. Plaintiff and Class Members have a reasonable expectation of privacy in their Private Information, including personal information and sensitive medical information.

118. HIPAA sets national standards for safeguarding protected health information. For example, HIPAA limits the permissible uses of health information and prohibits the disclosure of this information without explicit authorization. See 45 C.F.R. § 164.HIPAA also requires that covered entities implement appropriate safeguards to protect this information. See 45 C.F.R. § 164.530(c)(1).

119. Ther federal legal framework applies to health care providers, including Defendant.

120. Given the application of HIPAA to the Defendant, Plaintiff and the members of the Class had a reasonable expectation of privacy over their PHI.

121. Several studies examining the collection and disclosure of consumers' sensitive medical information confirm that the collection and unauthorized disclosure of sensitive medical information from millions of individuals, as Defendant have done here, violates expectations of privacy that have been established as general societal norms.

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

123. For example, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies and Website and Appss should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and Website and Appss should be required to provide consumers with a complete list of the data that has been collected about them.[38] Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[39]

124. Users act consistent with these preferences. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.[40]

125. Medical data is particularly even more valuable because unlike other personal information, such as credit card numbers which can be quickly changed, medical data is static. this is why companies possessing medical information, like Defendant, are intended targets of cyber-criminals.[41]

---

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

[39] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (November 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[40] Margaret Taylor, *How Apple Screwed Facebook*, WIRED (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[41] Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS (September 24, 2014), https://www.reuters.com/article/us-cybersecurity-

126. Patients using Defendant's Website and Apps must be able to trust that the information they input including their physicians, their health conditions and courses of treatment will be protected.

127. Indeed, numerous state and federal laws require this. And these laws are especially important when protecting individuals with particular medical conditions such as HIV or AIDS that can and do subject them to regular discrimination.

128. Furthermore, millions of Americans keep their health information private because it can become the cause of ridicule and discrimination. For instance, despite the anti-discrimination laws, persons living with HIV/AIDS are routinely subject to discrimination in healthcare, employment, and housing.[42]

129. The concern about sharing medical information is compounded by the reality that advertisers view this type of information as particularly high value. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born.

130. As one article put it: "the datafication of family life can begin from the moment in which a parent thinks about having a baby."[43] The article continues, "[c]hildren today are the very first generation of citizens to be datafied from before birth, and we cannot foresee —as yet— the social and political consequences of this historical transformation. What is particularly worrying about this process of datafication of children is that companies like . . . Facebook . . . are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[44]

---

hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

[42] Bebe J. Anderson, JD, *HIV Stigma and Discrimination Persist, Even in Health Care*, AMA J. ETHICS (December 2009), https://journalofethics.ama-assn.org/article/hiv-stigma-and-discrimination-persist-even-health-care/2009-12.

[43] Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, MIT PRESS READER (January 14, 2021), https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/.

[44] *Id.*

131. Other privacy law experts have expressed concerns about the disclosure to third parties of a users' sensitive medical information. For example, Dena Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra Labs—explained that having your personal health information disseminated in ways you are unaware of could have serious repercussions, including affecting your ability to obtain life insurance and how much you pay for that coverage, increase the rate you are charged on loans, and leave you vulnerable to workplace discrimination.[45]

132. Defendant surreptitiously collected and used Plaintiff's and Class Members' Private Information, including highly sensitive medical information, through tracking tools like Meta Pixel in violation of Plaintiff's and Class Members' privacy interests.

G. Defendant was Enriched & Benefitted from the Use of the Pixel & other Tracking Technologies that Enabled the Unauthorized Disclosures Alleged Herein.

133. Meta advertises its Pixel as a piece of code "that can help you better understand the effectiveness of your advertising and the actions people take on your site.... You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting…."[46]

134. Retargeting is a form of online marketing that targets users with ads based on previous internet communications and interactions. Retargeting operates through code and tracking pixels placed on a Website and Apps and cookies to track Website and Apps visitors and then places ads on other Website and Apps the visitor goes to later.[47]

---

[45] *See* Class Action Complaint, *Jane Doe v. Regents of the Univ. of Cal. d/b/a UCSF Medical Center*, CLASS ACTION (Feb. 9, 2023), https://www.classaction.org/media/doe-v-regents-of-the-university-of-california.pdf.

[46] *What is the Meta Pixel*, https://www.facebook.com/business/tools/meta-pixel (emphasis added) (last visited May 13, 2024).

[47] *The complex world of healthcare retargeting*, https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/ (last visited May 13, 2024).

135. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care Website and Apps back to Facebook via the tracking technologies and the Pixel embedded on, in this case, Defendant's Website and Apps.

136. Through this process, the Meta Pixel loads and captures as much data as possible when a User loads a healthcare Website and Apps that has installed the Pixel. The information the Pixel captures, "includes URL names of pages visited, and actions taken - all of which could be potential examples of health information."[48]

137. In exchange for disclosing the Private Information of their patients, Defendant was compensated by Facebook and likely other third parties in the form of enhanced advertising services and more cost-efficient marketing on their platform.

138. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many are not HIPAA-complaint or are only HIPAA-compliant if certain steps are taken.[49]

139. For example, Freshpaint a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant", and "If you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now."[50]

140. Medico Digital also warns that "retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences."[51]

141. Thus, utilizing the Pixels directly benefits Defendant by, among other things, reducing the cost of advertising and retargeting.

H. Plaintiff's & Class Members' Private Information Has Substantial Value.

---

[48] *Id*.

[49] *See* PIWIK Pro, *The guide to HIPAA compliance in analytics*, https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited Apr. 4, 2024).

[50] *Id*.

[51] *The complex world of healthcare retargeting*, *supra*, note 66.

142. Plaintiff's and Class Members' Private Information had value, and Defendant's disclosure and interception harmed Plaintiff and the Class by not compensating them for the value of their Private Information and in turn decreasing the value of their Private Information.

143. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the tech economy.

144. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[52] A 2015 article from TechCrunch accurately noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[53] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

145. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

146. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use.

147. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiff herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[54]

148. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

149. In 2023, the Value Examiner published a report that focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical

[52] *See The world's most valuable resource is no longer oil, but data*, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Apr. 4, 2024).

[53] *See* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited Apr. 4, 2024).

[54] *See 10 Apps for Seling Your Data for* Cash, https://wallethacks.com/apps-for-selling-your-data/ (last visited Apr. 4, 2024).

patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[55]

150. In 2021, Trustwave Global Security published a report entitled Hackers, breaches and the value of healthcare data. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[56]

151. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[57]

152. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[58]

153. The dramatic difference in the price of healthcare data when compared to other forms of private information that is commonly sold is evidence of the value of PHI.

154. But these rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

---

[55] *See Valuing Healthcare Data*, https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited Apr. 4, 2024).

[56] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (citing *The Value of Data*, https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf) (last visited Apr. 4, 2024).

[57] *See* https://time.com/4588104/medical-data-industry/ (last visited Apr. 4, 2024).

[58] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Apr. 4, 2024).

155. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

TOLLING, CONCEALMENT & ESTOPPEL

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

157. Defendant secretly incorporated the Meta Pixel into its Website and Apps and patient portals, providing no indication to Users that their User Data, including their Private Information, would be disclosed to unauthorized third parties.

158. Defendant had exclusive knowledge that the Meta Pixel was incorporated on its Website and Apps, yet failed to disclose that fact to Users, or inform them that by interacting with its Website and Apps, Plaintiff's and Class Members' User Data, including Private Information, would be disclosed to third parties, including Facebook.

159. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of Meta Pixels is highly technical and there were no disclosures or other indications that would inform a reasonable consumer that Defendant was disclosing and allowing Facebook to intercept Users' Private Information.

160. The earliest Plaintiff and Class Members could have known about Defendant's conduct was when Defendant announced this breach, in May of 2024. Nevertheless, at all material times herein, Defendant falsely represented to Plaintiff that their health information is not and will not be disclosed to any third party.

161. As alleged above, Defendant has a duty to disclose the nature and significance of its data disclosure practices but failed to do so. Defendant is therefore estopped from relying on any statute of limitations under the discovery rule.

CLASS ALLEGATIONS

162. **Class Definition:** Plaintiff bring this action on behalf of herself and on behalf of all others similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.:

163. The Nationwide Class that Plaintiff seek to represent is defined as:

> **Nationwide Class**: All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through tracking tools on the Defendant's Website and Apps.

164. The Nationwide Class, is referred to throughout this Complaint as the "Class."

165. **The following people are excluded from the Class:** (1) any Judge or Magistrate presiding over this action and members of their immediate families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

166. Plaintiff reserves the right under Federal Rule of Civil Procedure 23 to amend or modify the Class to include a broader scope, greater specificity, further division into subclasses, or limitations to particular issues. Plaintiff reserves the right under Federal Rule of Civil Procedure 23(c)(4) to seek certification of particular issues.

167. The requirements of Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3) are met in this case.

168. **Numerosity**: The exact number of Class Members is not available to Plaintiff, but it is clear that individual joinder is impracticable. Initial reports indicate that the potential Class size could be above 13,000,000 individuals.

169. **Commonality**: Commonality requires that the Class Members' claims depend upon a common contention such that determination of its truth or falsity will resolve an issue that is central to the validity of each claim in one stroke. Here, there is a common contention for all

Class Members as to whether Defendant disclosed to third parties their Private Information without authorization or lawful authority.

170. **Typicality**: Plaintiff's claims are typical of the claims of other Class Members in that Plaintiff and the Class Members sustained damages arising out of Defendant's uniform wrongful conduct and data sharing practices.

171. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff's claims are made in a representative capacity on behalf of the Class Members. Plaintiff has no interests antagonistic to the interests of the other Class Members. Plaintiff has retained competent counsel to prosecute the case on behalf of Plaintiff and the Class. Plaintiff and Plaintiff's counsel are committed to vigorously prosecuting this action on behalf of the Class members.

172. The declaratory and injunctive relief sought in this case includes:

a. Entering a declaratory judgment against Defendant—declaring that Defendant's interception of Plaintiff's and Class Members' Private Information is in violation of the law;

b. Entering an injunction against Defendant:

i. preventing Defendant from sharing Plaintiff's and Class Members' Private Information with third parties;

ii. requiring Defendant to alert and/or otherwise notify all Users of their Website and Apps of what information is being collected, used, and shared;

iii. requiring Defendant to provide clear information regarding practices concerning data collection from the Users/patients of Defendant's Website and Apps, as well as uses of such data;

iv. requiring Defendant to establish protocols intended to remove all personal information which has been leaked to Facebook and/or other third parties, and request Facebook/third parties to remove such information;

v. and requiring Defendant to provide an opt out procedure for individuals who do not wish for their information to be tracked while interacting with Defendant's Website and Apps.

173. **Predominance**: There are many questions of law and fact common to the claims of Plaintiff and Class Members, and those questions predominate over any questions that may affect individual Class Members. Common questions and/or issues for Class members include, but are not necessarily limited to the following:

a. Whether Defendant's unauthorized disclosure of Users' Private Information was negligent;

b. Whether Defendant owed a duty to Plaintiff and Class Members not to disclose their Private Information to unauthorized third parties;

c. Whether Defendant breached its duty to Plaintiff and Class Members not to disclose their Private Information to unauthorized third parties;

d. Whether Defendant represented to Plaintiff and the Class that they would protect Plaintiff's and the Class Members' Private Information;

e. Whether Defendant violated Plaintiff's and Class Members' privacy rights;

f. Whether Plaintiff and Class Members are entitled to actual damages, enhanced damages, statutory damages, and other monetary remedies provided by equity and law and

g. Whether injunctive and declaratory relief, restitution, disgorgement, and other equitable relief is warranted.

174. **Superiority:** this case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by individual Class Members will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual Class Members to obtain effective relief from Defendant's misconduct. Even if Class Members could mount such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort and expense will be enhanced, and uniformity of decisions ensured.

175. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant misrepresented that they would disclose personal information only for limited purposes that did not include purposes of delivering advertisements or collecting data for commercial use or supplementing consumer profiles created by data aggregators and advertisers;

b. Whether Defendant's privacy policies misrepresented that it collected and shared User information with third-party service providers only for the limited purpose of providing access to its services;

c. Whether Defendant misrepresented that they had in place contractual and technical protections that limit third-party use of User information and that it would seek User consent prior to sharing Private Information with third parties for purposes other than provision of its services;

d. Whether Defendant misrepresented that any information they receive is stored under the same guidelines as any health entity that is subject to the strict patient data sharing and protection practices set forth in the regulations propounded under HIPAA;

e. Whether Defendant misrepresented that they complied with HIPAA's requirements for protecting and handling Users' PHI;

f. Whether Defendant breached their contractual obligations to not share Users' PHI without express written authorization;

g. Whether Defendant shared the Private Information that Users provided to Defendant with advertising platforms, including Facebook, without adequate notification or disclosure, and without Users' consent, in violation of health privacy laws and rules and its own privacy policy;

h. Whether Defendant integrated third-party tracking tools, such as Pixels, in its Website and Apps that shared Private Information and User activities with third parties

for unrestricted purposes, which included advertising, data analytics, and other commercial purposes;

i. Whether Defendant shared Private Information and activity information with Facebook using Facebook's Pixels on its Website and Apps without Users' consent and

j. Whether Facebook used the information that Defendant shared with it for unrestricted purposes, such as selling targeted advertisements, data analytics, and other commercial purposes.

CLAIMS

COUNT ONE

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

18 U.S.C. § 2511(1), *et seq*.

Unauthorized Interception, Use and Disclosure

(*On Behalf of Plaintiff & the Nationwide Class*)

176. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

177. The ECPA prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

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

179. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

180. The transmissions of Plaintiff's PII and PHI to Defendant's Website and Apps qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

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

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

183. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiff and Class Members regarding PII and PHI, diagnosis of certain conditions, treatment/medication for such conditions, and scheduling of appointments, including annual mammograms, surgeries, ER visits, lab work, and scans.

184. Furthermore, Defendant intercepted the "contents" of Plaintiff's communications in at least the following forms:

a. The parties to the communications;

b. The precise text of patient search queries;

c. PII such as patients' IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;

185. For example, Defendant's interception of the fact that a patient views a webpage involves "content," because it communicates that patient's request for the information on that page.

186. **Interception**. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or

other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

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

a. The cookies Defendant and third parties used to track Plaintiff's and the Class Members' communications;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' computing devices

d. Defendant's web servers and

e. The Pixel code deployed by Defendant to effectuate the sending and acquisition of patient communications.

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

189. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via tracking tools, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Private Information to third parties such as Facebook.

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

191. This information was, in turn, used by third parties, such as Facebook to 1) place Plaintiff and Class Members in specific health-related categories and 2) target Plaintiff and Class Members with advertising associated with their specific health conditions.

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

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

194. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, violation of HIPAA and the causes of action described below, among others.

195. The ECPA provides that a "party to the communication" may liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

196. Defendant is not a party for purposes to the communication based on its unauthorized duplication and transmission of communications with Plaintiff and the Class. However, even assuming Defendant is a party, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

197. Here, as alleged above, Defendant violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing IIHI to a third party.

198. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

199. Plaintiff's and Class Members' information that Defendant disclosed to third parties qualifies as IIHI, and Defendant violated Plaintiff's expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant intentionally used the wire or electronic communications to intercept Plaintiff Private Information in violation of the law.

200. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it: Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and disclosed individually identifiable health information to third parties without patient authorization.

201. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

202. Defendant's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant's use of the tracking tools was for Defendant's commercial advantage to increase revenue from existing patients and gain new patients.

203. Defendant's acquisition of patient communications that were used and disclosed to Facebook was also done for purposes of committing criminal and tortious acts in violation of the laws of the United States and individual States nationwide as set forth herein, including:

a. Negligence;

b. Breach of express contract;

c. Breach of implied contract; and

d. Breach of fiduciary duty.

204. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiff's and Class Members' communications about their Private Information on its Website and Apps, because it used its participation in these communications to improperly share Plaintiff's and Class Members' Private Information with Facebook and third-parties that did not participate in these communications, that Plaintiff and Class Members did not know was receiving their information, and that Plaintiff and Class Members did not consent to receive this information.

205. Here, as alleged above, Defendant violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information to a third party.

206. As such, Defendant cannot viably claim any exception to ECPA liability.

207. Plaintiff and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

a. Learning that Defendant have intruded upon, intercepted, transmitted, shared, and used their PII and PHI for commercial purposes has caused Plaintiff and the Class Members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiff's and the Class Members' PII and PHI without providing any value or benefit to Plaintiff or the Class members;

c. Defendant received substantial, quantifiable value from their use of Plaintiff's and the Class Members' PII and PHI, such as understanding how people use its Website and Apps and determining what ads people see on its Website and Apps, without providing any value or benefit to Plaintiff or the Class Members;

d. Defendant have failed to provide Plaintiff and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of its patient information and

e. The diminution in value of Plaintiff's and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, medical treatment, and appointments that Plaintiff and Class Members intended to remain private no longer private.

208. Defendant intentionally used the wire or electronic communications to increase its profit margins.

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

210. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading their privacy.

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

212. Consumers have the right to rely upon the promises that companies make to them. Defendant accomplished its tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that caused third-party cookies and other tracking technologies to be deposited on Plaintiff's and Class members' computing devices as "first-party" cookies that are not blocked.

213. Defendant's scheme or artifice to defraud in this action consists of the false and misleading statements and omissions in its privacy policy set forth above, including the statements and omissions recited above; and

214. Defendant acted with the intent to defraud in that it willfully invaded and took Plaintiff's and Class Members' property:

a. property rights to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

b. property rights to determine who has access to their computing devices.

215. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Website and Apps, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

216. As a result of Defendant's violation of the ECPA, Plaintiff and the Class are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT TWO

BREACH OF EXPRESS CONTRACT

(On behalf of Plaintiff & the Nationwide Class)

217. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

218. Plaintiff and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with Defendant for the provision of medical and health care services.

219. Specifically, Plaintiff and Class Members entered into a valid and enforceable express contract with Defendant when Plaintiff first received medical care from Defendant.

220. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with Defendant include Defendant's promise to protect nonpublic, Private Information given to Defendant or that Defendant gathers on their own from disclosure.

221. Under these express contracts, Defendant and/or their affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

222. Both the provision of medical services and the protection of Plaintiff and Class Members' Private Information were material aspects of these express contracts.

223. The express contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

224. At all relevant times, Defendant expressly represented in its Privacy Notice, among other things, that it would protect Users' PII and PHI and not share it with third parties.

225. Defendant's express representations, including, but not limited to, express representations found in their Privacy Notice, formed and embodied an express contractual

obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

226. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

227. Plaintiff and Class Members would not have entered into these contracts with Defendant and/or their affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

228. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

229. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

230. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when it disclosed that Private Information to Meta through the Meta Collection Tools, including the Meta Pixel on its Website and Apps.

231. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by Defendant's sharing of that Private Information with third parties through tools embedded on its Website and Apps.

232. The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Meta, was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

233. As a result of Defendant's failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts.

234. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

235. Had Defendant disclosed that their data privacy was inadequate or that they did not adhere to industry-standard privacy measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or their affiliated healthcare providers.

236. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Meta, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

237. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Meta.

COUNT THREE

BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING

(On behalf of Plaintiff & the Nationwide Class)

238. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

239. Plaintiff and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with Defendant for the provision of medical and health care services.

240. Specifically, Plaintiff and Class Members entered into a valid and enforceable express contract with Defendant when Plaintiff first received medical care from Defendant.

241. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with Defendant include Defendant's implied duty of good faith and fair dealing, particularly due to Defendant's special relationship with Plaintiff as their healthcare provider.

242. Under these express contracts, Defendant and/or their affiliated healthcare providers, promised and were obligated to provide healthcare to Plaintiff and Class Members. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

243. In service of its implied duty of good faith and fair dealing when executing the contract, Defendant was bound to not voluntarily divulge Plaintiff's and Class Members' sensitive, non-public Private Information to third parties for monetary gain without Plaintiff's and Class Members' consent to such disclosures.

244. The express contracts for the provision of medical services are formed and embodied in multiple documents.

245. As evidence of Defendant's knowledge of its obligations to perform the contracts in accordance with its implied duty of good faith and fair dealing and Plaintiff's expectations of Defendant to do the same, at all relevant times, Defendant expressly represented in its Privacy Notice, among other things, that Defendant would safeguard Users' PHI and PII and not share it with third parties without consent.

246. Express representations found in their Privacy Notice evidence Defendant's knowledge of the specific manifestations of its duty to perform the contracts in accordance with its implied duty of good faith and fair dealing, which required Defendant to implement data

security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

247. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

248. Plaintiff and Class Members would not have entered into these contracts with Defendant and/or their affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

249. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and, through Defendant's implied duty of good faith and fair dealing, the protection of their Private Information.

250. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

251. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by Defendant's sharing of that Private Information with Meta through the Meta Collection Tools, including the Meta Pixel on its Website and Apps.

252. Defendant breached its implied duty of good faith and fair dealing to protect the nonpublic Private Information Defendant gathered when it disclosed that Private Information to third parties.

253. The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Meta, was a reasonably foreseeable consequence of Defendant's actions in breach of its implied duty of good faith and fair dealing.

254. As a result of Defendant's failure to fulfill the data privacy protections inherent in the special relationship with Plaintiff and the Class Members, and resulting breach of its implied duty of good faith and fair dealing, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts.

255. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

256. Had Defendant disclosed that their data privacy was inadequate or that they did not adhere to industry-standard privacy measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or their affiliated healthcare providers.

257. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Meta, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

258. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Meta.

COUNT FOUR

BREACH OF IMPLIED CONTRACT

(On behalf of Plaintiff & the Nationwide Class)

259. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

260. Plaintiff and Class Members allege they entered into valid and enforceable implied contracts or were third-party beneficiaries of valid and enforceable implied contracts, with Defendant for the provision of medical and health care services.

261. Specifically, Plaintiff and Class Members entered into a valid and enforceable contract with Defendant when Plaintiff first received medical care from Defendant.

262. The valid and enforceable contracts to provide medical and health care services that Plaintiff and Class Members entered into with Defendant include Defendant's promise to protect nonpublic, Private Information given to Defendant or that Defendant gathers on their own from disclosure.

263. Under these contracts, Defendant and/or their affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

264. Both the provision of medical services and the protection of Plaintiff and Class Members' Private Information were material aspects of these contracts.

265. The contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

266. Defendant's express representations, including, but not limited to, express representations found in their Privacy Notice, formed and embodied an express contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

267. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry

standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entered into these contracts with Defendant and/or their affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

268. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

269. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

270. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when it disclosed that Private Information to third parties.

271. Defendant materially breached the terms of these contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by Defendant's sharing of that Private Information with third parties.

272. The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Meta, was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

273. As a result of Defendant's failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

274. Had Defendant disclosed that their data privacy was inadequate or that they did not adhere to industry-standard privacy measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or their affiliated healthcare providers.

275. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Meta, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

276. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Meta.

COUNT FIVE

NEGLIGENCE

(On behalf of Plaintiff & the Nationwide Class)

277. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

278. Defendant required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare services.

279. Upon accepting, storing, and controlling the Private Information of Plaintiff and the Class in its computer systems, Defendant owed, and continues to owe, a duty to Plaintiff and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information from disclosure to third parties.

280. Defendant's duty of care to use reasonable measures to secure and safeguard Plaintiff's and Class Members' Private Information arose due, in part, to the special relationship

that existed between Defendant and its patients, which is recognized by statute, regulations, and the common law.

281. In addition, Defendant had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

282. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

283. Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

284. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

285. Defendant's duty to use reasonable care in protecting confidential data arose also because Defendant is bound by industry standards to protect confidential Private Information.

286. Defendant breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

287. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' Private Information through its use of the Meta Pixels and other tracking technologies would result in unauthorized third parties, such as Facebook, gaining access to such Private Information for no lawful purpose.

288. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information.

289. Defendant's misconduct included the failure to (1) secure Plaintiff's and Class Members' Private Information; (2) comply with industry standard data security practices; (3) implement adequate Website and Apps event monitoring; (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Meta Pixels and other tracking technologies; and (5) prevent unauthorized access to Plaintiff's and Class Members' Private Information by sharing that information with Meta and other third parties. Defendant's failures and breaches of these duties constituted negligence.

290. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and Class members' Private Information, Plaintiff and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

291. Defendant's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiff's and Class members' Private Information constituted (and continue to constitute) negligence at common law.

292. Plaintiff and Class Members are entitled to compensatory, nominal, and/or punitive damages, and Plaintiff and Class Members are entitled to recover those damages in an amount to be determined at trial.

293. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner. Therefore, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) cease sharing Plaintiff's and Class Members' Private Information with Meta and other third parties without Plaintiff's and Class Members'

express consent; and (iii) submit to future annual audits of its security systems and monitoring procedures.

COUNT SIX

BREACH OF FIDUCIARY DUTY

(On Behalf of Plaintiff & the Nationwide Class)

294. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

295. In light of the special physician-patient relationship between Defendant and Plaintiff and Class Members, which was created for the purpose of Defendant providing healthcare to Plaintiff and Class Members, Defendant became guardian of Plaintiff's and Class Members' Private Information. Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

296. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant' relationship with its patients and former patients, in particular, to keep secure their Private Information.

297. Defendant breached its fiduciary duties to Plaintiff and Class Members by disclosing their Private Information to unauthorized third parties, including Meta, and separately, by failing to notify Plaintiff and Class Members of this fact.

298. As a direct and proximate result of Defendant' breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injury and are entitled to compensatory, nominal, and/or punitive damages, and disgorgement of profits, in an amount to be proven at trial.

COUNT SEVEN

UNJUST ENRICHMENT

(On behalf of Plaintiff & Nationwide Class)

299. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein, except for the paragraphs specifically regarding breach of contract.

300. Plaintiff plead this claim in the alternative to their breach of contract claim.

301. Plaintiff and Class Members personally and directly conferred a benefit on Defendant by paying Defendant for health care services, which included Defendant's obligation to protect Plaintiff's and Class Members' Private Information. Defendant was aware of Plaintiff's privacy expectations, and in fact, promised to maintain Plaintiff's Private Information confidential and not to disclose to third parties. Defendant received payments for medical services from Plaintiff and Class Members.

302. Plaintiff and Class Members also conferred a benefit on Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiff and Class Members under the guise of keeping this information private.

303. Defendant collected, used, and disclosed this information for its own gain, including for advertisement, market research, sale, or trade for valuable benefits from Facebook and other third parties.

304. Defendant had knowledge that Plaintiff and Class Members had conferred this benefit on Defendant by interacting with its Website and Apps, and Defendant intentionally installed the Meta Pixel tool on its Website and Apps to capture and monetize this benefit conferred by Plaintiff and Class Members.

305. Plaintiff and Class Members would not have used Defendant's Website and Apps had they known that Defendant would collect, use, and disclose this information to Facebook, Google, and other third parties.

306. The services that Plaintiff and Class Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant

promised to provide, which included Defendant's promise that any patient communications with Defendant would be treated as confidential and would never be disclosed to third parties for marketing purposes without the express consent of patients.

307. The medical services that Defendant offers are available from many other health care systems that do protect the confidentiality of patient communications. Had Defendant disclosed that it would allow third parties to secretly collect Plaintiff's and Class Members' Private Health Information without consent, neither Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

308. By virtue of the unlawful, unfair and deceptive conduct alleged herein, Defendant knowingly realized hundreds of millions of dollars in revenue from the use of the Private Information of Plaintiff and Classes Members for profit by way of targeted advertising related to Users' respective medical conditions and treatments sought.

309. Ther Private Information, the value of the Private Information, and/or the attendant revenue, were monetary benefits conferred upon Defendant by Plaintiff and Class Members.

310. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in the loss of value of their Private Information and the lost profits from the use of their Private Information.

311. It would be inequitable and unjust to permit Defendant to retain the enormous economic benefits (financial and otherwise) it has obtained from and/or at the expense of Plaintiff and Class Members.

312. Defendant will be unjustly enriched if it is permitted to retain the economic benefits conferred upon them by Plaintiff and Class Members through Defendant's obtaining the Private Information and the value thereof, and profiting from the unlawful, unauthorized and impermissible use of the Private Information of Plaintiff and Class Members.

313. Plaintiff and Class Members are therefore entitled to recover the amounts realized by Defendant at the expense of Plaintiff and Class Members.

314. Plaintiff and the Class Members have no adequate remedy at law and are therefore entitled to restitution, disgorgement, and/or the imposition of a constructive trust to recover the amount of Defendant's ill-gotten gains, and/or other sums as may be just and equitable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of themselves and the Proposed Class defined herein, respectfully request this Honorable Court to provide the following relief:

A. That this Action be maintained as a Class Action, that Plaintiff be named as Class Representative of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order:

1. Preventing Defendant from sharing Plaintiff's and Class Members' Private Information among other third parties;

2. Requiring Defendant to alert and/or otherwise notify all Users of its Website and Apps of what information is being collected, used, and shared;

3. Requiring Defendant to provide clear information regarding its practices concerning data collection from the Users/patients of Defendant's Website and Apps, as well as uses of such data;

4. Requiring Defendant to establish protocols intended to remove all personal information which has been leaked to Facebook and/or other third parties, and request Facebook/third parties to remove such information;

5. Requiring Defendant to provide an opt out procedure for individuals who do not wish for their information to be tracked while interacting with Defendant's Website and Apps;

6. Mandating the proper notice be sent to all affected individuals, and posted publicly;

7. Requiring Defendant to delete, destroy, and purge the Private Information of Users unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Users;

8. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

C. That the Court award Plaintiff and the Class Members damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

D. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiff and the Class are entitled, including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

E. Plaintiff and the Class be awarded with pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

F. Plaintiff and the Class be awarded with the reasonable attorneys' fees and costs of suit incurred by their attorneys;

G. Plaintiff and the Class be awarded with treble and/or punitive damages insofar as they are allowed by applicable laws; and

H. Any and all other such relief as the Court may deem just and proper under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all claims so triable.

Dated: June 4, 2024

By: */s/ Robert Mackey*

Robert Mackey (SBN 125961)
bobmackeyesq@aol.com
LAW OFFICES OF ROBERT MACKEY
16320 Murphy Road,
Sonora, CA 95370
Tel: (412) 370-9110

Jason S. Rathod*
jrathod@classlawdc.com
MIGLIACCIO & RATHOD LLP
412 H Street NE, no. 302,
Washington, DC, 20002
Office: (202) 470-3520

* *pro hac vice* forthcoming

Attorneys for Plaintiffs and the Proposed Class

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Alexis Sutter

(b) County of Residence of First Listed Plaintiff Fairfax
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Robert Mackey, 16320 Murphy Road, Sonora, CA 95370, (412) 370-9110

DEFENDANTS

KAISER FOUNDATION HEALTH PLAN, INC.

County of Residence of First Listed Defendant Alameda
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent—Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation–Transfer ☐ 8 Multidistrict Litigation–Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
18 U.S.C. § 2511(1), et seq.

Brief description of cause:
Unauthorized Interception, Use and Disclosure, Breach of Express Contract

VII. REQUESTED IN COMPLAINT:

☑ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S), IF ANY *(See instructions):*

JUDGE Jon S. Tigar DOCKET NUMBER 4:24cv1426

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 06/04/2024 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Robert A. Mackey

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. Jurisdiction. The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked**.** (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

Date and Attorney Signature. Date and sign the civil cover sheet.