LYNCH CARPENTER, LLP
(Eddie) Jae K. Kim (SBN: 236805)
ekim@lcllp.com
Tiffine E. Malamphy (SBN 312239)
tiffine@lcllp.com
117 E Colorado Blvd, Ste 600
Pasadena, CA 91105-3712
Tel.: (213) 723-0707
Fax: (858) 313-1850

Attorneys for Plaintiff
and Proposed Class Counsel

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

AUSTIN KAHN, on behalf of himself and all others similarly situated, Plaintiff, v. CALIFORNIA PHYSICIANS' SERVICE, D/B/A BLUE SHIELD OF CALIFORNIA, Defendant.	Case No.: **CLASS ACTION COMPLAINT**

Plaintiff Austin Kahn ("Plaintiff"), on behalf of himself and all others similarly situated, asserts that following against Defendant California Physicians' Service d/b/a Blue Shield of California ("Blue Shield" or "Defendant"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel:

NATURE OF THE ACTION

1. Plaintiff brings this case to address Defendant's unlawful practice of disclosing Plaintiff's and Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Personal Health Information") to Google LLC ("Google"), without their knowledge or consent.

2. Blue Shield is a health insurance company that offers health plans to approximately six million health plan members.

3. Defendant owns and controls the website and subpages located at www.blueshieldca.com ("Website"), which it encourages patients to "Find a doctor," navigate resources to find care options for specific illnesses and conditions, compare prices for specific prescription drugs, access and upload sensitive financial and medical documents, and download "self-guided" resources to treat mental health conditions, among other functions.

4. As a health insurance provider, Blue Shield is a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA") and is required by law to provide every member with a Notice of Privacy Practices. Defendant's HIPAA Privacy Notice states that "[w]e are required to maintain the privacy of your PHI [personal health information]." Defendant further explains that it may only disclose PHI without written authorization for a limited enumerated purposes, and that "[w]e will not use your PHI for marketing purposes without your prior written authorization."[1]

5. Indeed, information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences. [2]

6. Despite Blue Shield's duty to safeguard and keep confidential its patients' Personal Health Information, Blue Shield nevertheless intentionally chose to procure and embed third-party tracking technologies on its website, disclosing information about its members—including their physicians, their medical treatments, the hospitals they visited, and their personal identities—to Google without patients' knowledge, authorization, or consent.

[1] Notice of Privacy Practices, Blue Shield of California, *available at* https://www.blueshieldca.com/content/dam/bsca/en/member/docs/2024/C18305-0923-REF1520344-SECURE.pdf (last updated August 16, 2013).

[2] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022), *available at* https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized."); *see also* Todd Feathers et al, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022), *available at* https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

7. The disclosure of Plaintiff's and Class Members' Personal Health Information enabled Google to gain deep insights into the types of medical conditions afflicting Defendant's members as well as the types of medical care and medical treatments patients sought from health care providers.

8. On April 9, 2025, Blue Shield published a page on the Website ("Data Incident Notice") notifying its members of a purported data breach.[3] However, the Data Incident Notice does not describe a conventional data breach, *i.e.* a "security incident in which unauthorized parties access sensitive or confidential information."[4] Indeed, Blue Shield maintains that "no bad actor was involved" in the incident.[5]

9. Instead, the Data Incident Notice informs Blue Shield's members, including Plaintiff and Class Members, that Blue Shield has been intentionally and *voluntarily* disclosing their Personal Health Information to Google for years.

10. As described throughout this Complaint, Blue Shield did not reasonably protect, secure or store Plaintiff's and Class Members' Personal Health Information, but rather intentionally and knowingly granted Google access to confidential member information that Blue Shield knew or should have known was unlawful.

11. Blue Shield's actions constitute a disregard for the privacy of its members' Personal Health Information, and its duties as a health insurance provider and HIPAA covered entity, and its actions further constitute an invasion of Plaintiff's and Class Members' right to privacy, and violate federal and state statutory law and common law.

PARTIES

12. Plaintiff Austin Kahn is a natural person and citizen of California where he intends to remain.

13. Defendant California Physicians' Service d/b/a Blue Shield of California is a corporation organized under California law with its primary place of business at 601 12th Street, Oakland, California.

---

[3] Notice of Data Breach, Blue Shield of California (April 9, 2025), https://news.blueshieldca.com/notice-of-data-breach (last accessed April 14, 2025).

[4] *See, e.g., What is a data breach?*, IBM (May 4, 2024), https://www.ibm.com/think/topics/data-breach (last accessed April 14, 2025).

[5] Notice of Data Breach, *supra* note 4.

JURISDICTION & VENUE

14. This Court has federal question subject matter jurisdiction under 28 U.S.C. § 1331 because this suit is brought under the laws of the United States (18 U.S.C. §§ 2510, *et seq.*).

15. This Court has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

16. In the alternative, this Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this case is brought as a class action where the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendant.

17. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

18. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL BACKGROUND

A. How Google Analytics Works

19. Google markets Google Analytics as a platform that offers "a complete understanding of your customers across devices and platforms" to "understand the customer journey and improve marketing ROI [return on investment]."[6]

20. Google Analytics has been described by the Wall Street Journal as "far and away the web's most dominant analytics platform," which "tracks you whether or not you are logged in."[7]

21. When a user accesses a website utilizing Google Analytics, Google's code surreptitiously directs the user's browser to duplicate the communication with the host website and concurrently send that message to Google's servers.

[6] *Marketing Platform: Analytics*, Google, https://marketingplatform.google.com/about/analytics/ (last accessed April 15, 2025).

[7] https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401

22. In essence, Google Analytics code intercepts a user's interactions in real-time as the user navigates the page. That includes intercepting any information that the user may input, such as the text of search terms, links that the user clicked, files a user downloads, and even the amount of time a user spends engaging with a webpage.

23. Google Analytics contemporaneously sends a second, duplicate set of transmissions to Google's servers. Those duplicated transmissions are initiated by Google Analytics code and are concurrent with the communications with the host website, enabling Google instantaneously to collect and view the same information that website users are sharing with the host, *i.e.*, Blue Shield's own website.

24. The Google Analytics measurement code also collects information from the browser, such as the language setting, the type of browser and the device and operating system on which the browser is running. It even can collect and record the "traffic source" – which is what brought the user to the site in the first place – such as a search engine, an advertisement on which the user clicked, or an email marketing campaign.[8]

25. To begin tracking website users as described above, a website operator like Blue Shield creates a Google Analytics account and then embeds small piece of JavaScript measurement code ("Google Tag") to every page on the website. Once these two steps are complete, Google immediately begins duplicating and intercepting users' website communications as described above.

26. All the information collected by the Google Analytics JavaScript code, while it also is in transit to the host website, is sent simultaneously to Google for processing. Once Google Analytics receives, views, reads, and processes the raw user data, it aggregates and organizes the data based on particular criteria.

27. The website operator then has access to the Google Analytics console, where Google hosts data about users' website activity, and organizes data into analytics reports. Those reports include reports on acquisition (e.g., information about where the traffic originated and the methods by which users arrived at a site), engagement (what web pages and app screens a user visited), and demographics

[8] *How Google Analytics Works*, Google Analytics Help, https://support.google.com/analytics/answer/12159447 (last accessed April 15, 2025).

(a user's age, location, language, gender, and interests expressed when browsing online and engaging in purchase activities). The website operator can also create custom filters and data views to aggregate usage data into customized reports.

28. In addition to accessing and using the data collected from website users to provide its services, Google also uses the information shared by websites like Blue Shield to maintain and improve Google's own services, develop new services, measure the effectiveness of its advertising, and personalize content and ads that one sees on Google and its partners' websites and applications.

29. As Google represents to website operators, the true value of digital analytics comes from measuring consumer engagement for marketing purposes. This is why Google recommends that website operators "[p]ut your insights from Google Analytics to work with Google Ads to help get your business in front of the right customers…."[9]

30. Google Ads is a Google's online advertising program, which allows website owners to "create online ads to reach people exactly when they're interested in the products and services that you offer."[10] Google Ads works by targeting users based on information gathered by or inferred from data sources such as Google Analytics.

31. In its default configuration, Google Analytics is not connected to Google Ads. To begin feeding user data to Google Ads, a website operator like Blue Shield must first set up a Google Ads account; link its Google Ads account to the Google Analytics account; and import site metrics from its Google Analytics account into its Google Ads account.[11]

32. Google warns web developers that Google marketing tools, like Google Analytics and Google Ads, are not appropriate for health-related webpages and websites. Indeed, Google warns web developers that "Health" is a prohibited category that should not be used by advertisers to target ads to users or promote advertisers' products or services.

[9] *The Value of Digital Analytics*, Google, https://support.google.com/analytics/answer/12159453 (last accessed April 14, 2025).

[10] *How to be successful with Google Ads*, https://support.google.com/google-ads/answer/6080949 (last accessed April 14, 2025).

[11] *See, e.g., [UA] Product Linking: Link a Google Analytics (Universal Analytics) property to Google Ads [Legacy]*, https://support.google.com/google-ads/answer/1704341 (last accessed April 14, 2025).

B. Blue Shield Intentionally Procured and Embedded Google Analytics and Google Ads Functionality on its Website.

33. Blue Shield is a health plan with 4.8 million members and over $25 billion in annual revenue.[12] However, Blue Shield lost its state-tax exempt status in March 2015 when it was revoked by the California Franchise Tax Board.

34. Blue Shield operates the website and subpages of https://www.blueshieldca.com. Blue Shield's website enables members to "Find a doctor," navigate resources to find care options for specific illnesses and conditions, compare prices for specific prescription drugs, access and upload sensitive financial and medical documents, and download "self-guided" resources to treat mental health conditions, among other functions.

35. As a health insurance provider, Blue Shield has fiduciary, common law, and statutory duties to protect the confidentiality of member information and communications. Despite these duties however, Blue Shield intentionally procured and embedded tracking technologies on its website and related subpages that disclosed Plaintiff's and Class Members' Personal Health Information without their knowledge or consent.

36. In defiance of Google's warning about the dangers of using Google Analytics on sites hosting health-related communications, Blue Shield intentionally employed Google tracking tools on its health-related Website and subpages, resulting in the transmission of Personal Health Information communicated on the Website to Google Analytics and Google Ads.

37. Since approximately November 2013, Blue Shield has procured and embedded Google Tags on its website to power Google Analytics. During this time, Google Analytics tracked members' website activities and simultaneously disclosed that information to Google, who could then use the harvested information to infer intimate details about members' health.

38. Blue Shield installed Google Tags on its Website and thereby routinely disclosed details about members website activity, including Personal Health Information that is captured by Google Analytics and simultaneously disclosed, to Google.

---

[12] *Leading the Way Well Ahead: 2023 Mission Report*, Blue Shield of California, https://www.blueshieldca.com/content/dam/bsca/en/member/docs/Blue-Shield-of-California-2023-Mission-Report.pdf at 4 (last accessed April 14, 2025).

39. Transmissions of Personal Health Information occur simultaneously with members' communications with Defendant and include communications that Plaintiff and Class Members made about specific medical providers, treatments, conditions, appointments, payments, and registrations and logins to Defendant's member portal.

40. Upon information and belief, the tracking technologies procured and embedded on Blue Shield's website and related subpages intercepted and disclosed sensitive and non-public Personal Health Information to Google.

41. In fact, in the Data Incident Notice, Blue Shield admitted that information disclosed to Google "likely" included information such as:

a. Plaintiff's and Class Member's names, cities, zip codes, genders, and family sizes;

b. Plaintiff's and Class Members' insurance plan names, types, and group numbers, and other financial responsibility information;

c. Plaintiff's and Class Members' online member account identifiers;

d. Plaintiff's and Class Member's medical claim service dates and medical providers; and

e. Plaintiff's and Class Members' search inputs for Blue Shield's "Find a Doctor" feature and search results including the location, plan name and type, and provider name and type.

42. Blue Shield also admitted that "between April 2021 and January 2024, Google Analytics was configured in a way that allowed certain member data to be shared with Google's advertising product, Google Ads."[13]

43. However, as described above, data from Google Analytics is not shared with Google Ads unless the website operator—Blue Shield—takes affirmative steps to create a Google Ads account and to connect the two products.

[13] Notice of Data Breach, *supra* note 4.

44. The Data Incident Notice thus attempts to conceal Blue Shield's active and intentional role in gathering members' Personal Health Information and disclosing it to Google for use in targeted advertising campaigns.

45. The Data Incident Notice represents that Blue Shield only "discovered" that it was sending members' Personal Health Information to Google Ads on February 11, 2025, and "immediately initiated a review of its websites and security protocols."[14]

46. But elsewhere in the Data Incident Notice, Blue Shield asserts that it "severed the connection between Google Analytics and Google Ads on its websites in January 2024."[15] Blue Shield never explains how it severed this connection thirteen months *before* it was discovered. Nor does Blue Shield explain why it waited until April 2025—fifteen months after the connection to Google Ads was purportedly severed—to alert Plaintiff and Class Members that their Personal Health Information was compromised.

47. Nevertheless, Blue Shield's Data Incident Notice reflects a mistaken assumption that only its disclosures to Google Ads violated Plaintiff's and Class Members' privacy rights under common and statutory law.

48. In fact, Blue Shield's disclosures of Personal Health Information to Google Analytics—*which continue to this day*—also violate Plaintiff's and Class Members' privacy rights under common and statutory law.

49. Blue Shield interfered with Plaintiff's and Class Members' privacy rights when it implemented tracking technology (including Google Analytics and Google Ads) that surreptitiously tracked, recorded, and disclosed Plaintiff's and Class Members' confidential information to Google.

50. Blue Shield also breached its obligations to Plaintiff and Class Members in multiple other ways, including (1) failing to obtain their consent to disclose their private information to Google, (2) failing to adequately review its marketing programs and web-based technology to ensure its website was safe and secure, (3) installing software code that was known and designed to share members' private information with third parties, (4) failing to take steps to block the transmission of Plaintiff's and Class

[14] Notice of Data Breach, *supra* note 4.

[15] Notice of Data Breach, *supra* note 4.

Members' private information to Google, (5) failing to warn Plaintiff and Class Members that Blue Shield was routinely bartering their private information to Google, and (6) otherwise ignoring Blue Shield's common and statutory obligations to protect the confidentiality of patients' protected health information.

51. Plaintiff and Class Members have suffered injury because of Blue Shield's conduct. Their injuries include invasion of privacy and the continued and ongoing risk of irreparable harm from the disclosure of their most sensitive and personal information.

C. The Nature of Defendant's Unauthorized Disclosure of Health Information to Google.

52. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accessed web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

53. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

54. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses. Any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies[16]:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies. POST Requests are a separate type of HTTP Request that can send a large amount of data outside of the URL (*e.g.*, uploading a PDF to a court's ECF system for filing a motion).

[16] "Cookies are small files of information that a web server generates and sends to a web browser. …Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Apr. 5, 2023).

- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies that have been placed on the client device are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data to the cookie owner's website when the user is visiting an entirely different website.
- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.[17] HTTP Responses can also send cookies or other code hidden and embedded in the webpage to the client device's browser.

55. When an individual visits Defendant's Website, an HTTP Request is sent from that individual's web browser to Defendant's servers that essentially asks Defendant's Website to retrieve certain information (such as Defendant's "Schedule Appointment Now" page). The HTTP Response from Defendant's servers sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Website.

56. Every website is comprised of Markup and "Source Code." Source Code is simply 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.

57. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's customized implementation of the Google Tags is source code that does just that. The Google Tag acts much like a traditional wiretap. When members visit Defendant's website via an HTTP Request to Defendant's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user along with Source Code that includes the Google Tags that power Google's marketing services, including Google Analytics and Google Ads. In essence, Defendant

[17] One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

is handing members a bugged phone. Once the Webpage loads in the members browser, the software-based wiretap quietly waits for a communication from the member to trigger the tap, which intercepts those communications intended only for Defendant and transmits them to Google.

58. The inclusion of Google Tags on a website does not provide any substantive content to the website user. In other words, Google does not provide anything to the user, but only serves to track user data and communications to further the marketing purposes of the website owner (*i.e.,* to bolster profits).

59. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer its members' computing devices, causing the device's web browser to contemporaneously and invisibly re-direct the members' communications to hidden third parties like Google.

60. In this case, Defendant employed Google Tags to intercept, duplicate, and re-direct Plaintiff's and Class Members' Personal Health Information to Google and its Google Analytics and Google Ads products.

61. The member visiting Defendant's Website only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

62. The Google Tag is embedded in Defendant's Source Code contained in its HTTP Response. The Google Tag, programmed to automatically track and transmit the members' communications with Defendant's Website to Google, executes instructions that effectively open a hidden spying window into the patient's browser through which Google can intercept the visitor's data, actions, and communications with Defendant.

63. Defendant's Source Code manipulates the members' browser by secretly instructing it to duplicate the members' communications (HTTP Requests) with Defendant and to send those communications to Google. These transmissions occur contemporaneously, invisibly, and without the patient's knowledge.

64. Thus, without its members' consent, Defendant has effectively used its source code to commandeer and "bug" or "tap" its members' computing devices, allowing Google and other third

parties to listen in on all of their communications with Defendant and thereby intercept those communications, including Personal Health Information.

65. Consequently, when Plaintiff and Class Members visit Defendant's website and communicate their Personal Health Information, including, but not limited to, precise text of search queries about specific doctors and prescription drugs; users' downloads of information about specific illnesses, conditions, and mental health disorders; summaries of communications between patients and Blue Shield; these communications are simultaneously intercepted and transmitted to Google.

66. Google tracks internet users with IP addresses, cookies, geolocation, and other unique device identifiers.

67. Google cookies are personally identifiable. For example, Google cookies called 'SID' and 'HSID' contain digitally signed and encrypted records of a user's Google account ID and most recent sign-in time.

68. Most people who use Google services have a preferences cookie called 'NID' in their browsers. When a user visits a Google service, the browser sends this cookie with your request for a page. The NID cookie contains a unique ID Google uses to remember user preferences and other information.

69. Google uses cookies like NID and SID to help customize ads on Google properties, like Google Search. For example, Google uses such cookies to remember users' most recent searches, previous interactions with an advertiser's ads or search results, and visits to an advertiser's website. This helps Google show customized ads to users on Google.

70. Google also uses one or more cookies for advertising it serves across the web. One of the main advertising cookies on non-Google sites is named 'IDE' and is stored in browsers under the domain doubleclick.net. Another is stored in google.com and is called ANID. Google also uses other cookies with names such as DSID, FLC, AID, TAID, and exchange_uid. Other Google properties, like YouTube, may also use these cookies to show users ads.

71. Google's ability to track specific individual users is no secret; in fact, the power to identify users and place them in "target audiences" for marketing purposes is a core element of Google Analytics. Google suggests configuring target audiences based on criteria such as, for

example,"[p]urchasers who were once active, but have not been active for the last 7 days," or "[u]sers who were once active, but have not been active for the last 7 days,"[18] audiences whose members would be impossible to ascertain without data to track and identify specific individual users.

72. Google cookies thus provide personally identifiable data about patients who visit Blue Shield's website to Google, and Blue Shield transmits personally identifiable Google cookie data to Google.

73. Accordingly, Google receives patients' communications alongside the patients' IP address, which is also impermissible under HIPAA.

D. Blue Shield Exploited Plaintiff's and Class Members' Personal Health Information for Financial Gain.

74. A website that incorporates Google Analytics and Google Ads benefits from the ability to analyze a user's experience and activity on the website to assess the website's functionality and traffic. The website also gains information from its customers that can be used to target them with advertisements, as well as to measure the results of advertising efforts.

75. Google's intrusion into the personal data of visitors to third-party websites incorporating Google code is both significant and unprecedented. When Google Analytics and/or Google Ads are incorporated into a third-party website, unbeknownst to users and without their consent, Google gains the ability to surreptitiously gather every user interaction with the website ranging from what the user clicks on to the personal information entered on a website search bar. Google aggregates this data against all websites. Google benefits from obtaining this information because it improves its advertising network, including its machine-learning algorithms and its ability to identify and target users with ads.

76. Google provides websites using Google Analytics with the data it captures in a reporting console, and Google Ads offers tools and analytics to reach these individuals through future online advertising. For example, websites can use this data to create "custom audiences" to target the specific user as well as other users who match "custom audience's" criteria. Businesses that use Google

[18] *See, e.g., Suggested Audiences*, Google Analytics Help, https://support.google.com/analytics/answer/10427338 (last accessed April 18, 2025).

Analytics and Google Ads can also process, filter, and search through data to find specific types of users to target, such as men over a certain age.

77. Unsurprisingly, Google does not offer its Tags, Analytics, and Ads products to companies like Defendant solely for Defendant's benefit. Google has built its nearly-$2 trillion market capitalization on mining and processing data to drive targeted advertising. Google's advertising services alone generate about 80 percent of the company's revenue—about $150 million annually.[19] The large volumes of personal and sensitive health-related data Defendant intentionally disclosed to Google are actively viewed, examined, analyzed, curated, and put to use by the company. Google acquires the raw data to transform it into a monetizable commodity, just as an oil company acquires crude oil to transform it into gasoline. Indeed, website operators can implement a baseline version of Google Analytics free of charge, "paying" for the service by allowing Google to collect website users' data.

78. Google sells advertising space by emphasizing its ability to target users. Google is especially effective at targeting users because it surveils user activity both on and off its site (with the help of companies like Defendant). This allows Google to make inferences about users beyond what they explicitly disclose. Advertisers can then use this data to apply highly specific filters and parameters for their targeted advertisements.

79. Google does not merely collect information gathered by the Google Tags and store it for safekeeping on its servers without ever viewing or accessing the information. Instead, in accordance with the purpose of Google Analytics and Google Ads to aggregate data for advertising and marketing purposes, Google viewed, processed, and analyzed Plaintiff; and Class Members' confidential Personal Health Information. Upon information and belief, such viewing, processing, and analyzing was performed by computers and/or algorithms programmed and designed by Google employees at the direction and behest of Google.

[19] Megan Graham, *How Google's $150 billion advertising business works*, CNBC (last updated Oct. 13, 2021), https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html (last accessed April 14, 2025).

80. Google receives over 20 petabytes[20] of information every day and must rely on analytical tools designed to view, categorize, and extrapolate the data to augment human effort.[21] This process, known as data ingestion, allows businesses to manage and make sense of large amounts of data.

81. By using data ingestion tools, Google is able to rapidly translate the information it receives from Google Tags in order to display relevant ads to consumers. For example, if a consumer visits a retailer's webpage and places an item in their shopping cart without purchasing it, the consumer will consistently receive targeted ads for that item as they browse the internet. This evidences that Google views and categorizes data as they are received from Google Tags.

82. Moreover, even if Google eventually deletes or anonymizes Personal Health Information that it receives, it must first view that information in order to identify it as containing Personal Health Information suitable for removal. Accordingly, there is a breach of confidentiality the instant the information is disclosed or received without authorization. As described by the Department of Health & Human Services:

> It is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed [business associate agreement] in place and requires that there is an applicable Privacy Rule permission for disclosure.[22]

E. Plaintiff had his Personal Health Information Intercepted, Disclosed, and Exploited by Defendant

83. Blue Shield facilitated the interception of Plaintiff's Personal Health Information, including sensitive medical information, to Google without his consent or authorization when he entered information on the websites that Blue Shield maintains. The information that Plaintiff transmitted included queries about potential doctors and treatments for his medical conditions.

---

[20] A petabyte is equal to one million gigabytes (1,000,000 GB).

[21] *Breaking Down the Numbers: How Much Data Does the World Create Daily in 2024?*, Edge Delta (Mar. 11, 2024), https://edgedelta.com/company/blog/how-much-data-is-created-per-day (last accessed April 18, 2025).

[22] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dept. of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last accessed April 15, 2025.

84. Plaintiff is a Blue Shield member who has received treatment covered by his Blue Shield insurance plan for a variety of medical conditions over the past decade. During that time, Plaintiff has regularly used Defendant's Website and has communicated his personal and medical information, including information relating to his medical conditions and treatments.

85. Unbeknownst to Plaintiff, Blue Shield had installed Google tracking technologies on the Website. This resulted in the disclosure of Plaintiff's Personal Health Information to Google without his consent.

86. After using the Blue Shield Website, Plaintiff began receiving targeted advertising that was directly related to his interactions on the Blue Shield Website and the medical conditions for which he sought treatment.

87. Plaintiff never consented to the use of his Personal Health Information by third parties or to Defendant enabling third parties—like Google—to access or interpret such information.

88. Plaintiff reasonably believed that his interactions with Blue Shield's website and member portal were private and would not be shared with any third party for marketing or advertising purposes. But for his status as a member of Defendant's health insurance plan, Plaintiff would not have disclosed any of his Personal Health Information to Defendant. Plaintiff was dismayed and outraged when he learned that Blue Shield's website had been capturing his Personal Health Information and disclosing that information to Google without his consent.

F. Defendant's Interception Occurred Without Plaintiff's or Class Members' Knowledge or Consent

89. Plaintiff and Class Members had no idea when they interacted with Blue Shield's websites that their personal data, including sensitive medical data, was being collected and simultaneously transmitted to Google. That is because, among other things, the Google Tags that power Google Analytics and Google Ads functionality are secretively and seamlessly integrated into Blue Shield's Website and is invisible to patients visiting the Website.

90. For instance, when Plaintiff and Class Members visited Blue Shield's Website, there was no indication that Google Analytics or Google Ads had been enabled on the Website, or that Blue Shield was actively disclosing Plaintiff's communications with the Website to Google in real-time.

91. Blue Shield's HIPAA Privacy Notice does not furnish consent to share Plaintiff's and Class Members' Personal Health Information with Google. Blue Shield's HIPAA Privacy Practice expressly states that "we will not use your PHI for marketing purposes without your prior written authorization."[23]

92. In any event, Blue Shield, as a covered entity under HIPAA, does not have a legal right to share Plaintiff's and Class Members' Protected Health Information without their written consent to third parties, because this information is protected from such disclosure by law. 45 C.F.R. § 164.508.

93. The HIPAA Privacy Rule, located at 45 C.F.R. Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[24]

94. The Privacy Rule broadly defines "protected health information" as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

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

96. Under the HIPPA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient

[23] HIPAA Privacy Notice, supra note 4.

[24] *The HIPAA Privacy Rule*, U.S. Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last accessed April 15, 2025).

to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

a. Names;

***

H. Medical record numbers;

***

J. Account numbers;

***

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers; … and

R. Any other unique identifying number, characteristic, or code…;and"

The covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 160.514.

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

98. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6.

99. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Advocate when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

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

101. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[25]

102. In its guidance for Marketing, the Department further instructs:

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

103. In December 2022, the HHS issued a bulletin reminding healthcare providers that hospitals are prohibited from transmitting individually identifiable health information via tracking

[25] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. Dept. of Health & Human Services, (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last accessed April 15, 2025).

[26] *OCR HIPAA Privacy: Marketing*, U.S. Dept. of Health & Human Services (Dec. 3, 2002), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last accessed April 15, 2025) (emphasis added).

technology without a patient's authorization and other protections like a business associate agreement with the recipient of the patient data:

> 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]

104. As the bulletin makes clear, the disclosure of Plaintiff's and Class Members' Personal Health Information via Google Tags contravenes both the letter and spirit of HIPAA's "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") which governs how health care providers must safeguard and protect Personal Health Information.

105. The bulletin also discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or other. For example, an impermissible disclosure of PHI 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 other identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.[28]

106. Plaintiff and Class Members face the same risks the government is warning about. Defendants have shared Plaintiff's and Class Members' search terms about health conditions for which they seek doctors; their contacts with doctors to make appointments; the names of their doctors; the frequency with which they take steps to obtain treatment for certain conditions; and where they seek medical treatment. This information is, as described by the OCR bulletin, "highly sensitive." The Bulletin goes on to make clear how broad the government's view of protected information is.

---

[27] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dept. of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last accessed April 15, 2025).

[28] *Id.*

107. This information 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, medical device IDs, or any unique identifying code.

108. Crucially, that paragraph in the government's Bulletin continues:

> All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website 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 IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.[29]

109. Likewise, after it became public knowledge that healthcare companies had been sharing their customers' medical information with third parties via tracking technologies, the FTC instituted a series of enforcement actions, including lawsuits against BetterHelp, GoodRx, Premom, and Vitagene. These lawsuits, which resulted healthcare companies paying millions of dollars in fines, underscore that HIPAA covered entities violate federal law by failing "to get consumers' affirmative express consent for the disclosure of sensitive health information."[30]

110. In July 2023, the HHS and the FTC issued a joint letter to approximately 130 hospitals to emphasize the risks and concerns about the use of technologies, such as Google Analytics, which can track a user's online activities. The joint letter emphasized the HHS and the FTC's concerns about the "serious privacy and security risks related to the use of online tracking technologies" on websites that "impermissibly disclos[e] consumers' sensitive personal healthy information to third parties."[31] As the agencies noted in an accompanying press release, "When consumers visit a hospital's website or seek

---

[29] *Id.*

[30] *Protecting the privacy of health information: A baker's dozen takeaways from FTC Cases,* Federal Trade Com'n (July 25, 2023), https://web.archive.org/web/20250310234552/https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (archived March 10, 2025).

[31] *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies,* Federal Trade Com'n (July 20, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking (last accessed April 15, 2025).

telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties."[32]

111. Defendant failed to obtain a valid written authorization from Plaintiff or any of the Class Members to allow the capture and exploitation of their personally identifiable information and the contents of their communications by third parties for their own direct marketing uses. Moreover, no additional privacy breach by Google is necessary for harm to have accrued to Plaintiff and Class Members; the secret disclosure by Defendant of its members' Personal Health Information to Google means that a significant privacy injury has already occurred.

112. Blue Shield failed to obtain a valid written authorization from Plaintiff or any of the Class Members to allow the capture and exploitation of their personally identifiable information and the contents of their communications for marketing purposes.

113. Neither Plaintiff nor Class Members knowingly consented to Defendant's disclosure of their Personal Health Information to Google. Nowhere on its website does Defendant tell members that it routinely shares their Personal Health Information with Google. Without disclosing such practices, Defendant cannot have secured consent from Plaintiff and Class Members for the disclosure of their Personal Health Information to Google or any other third-party advertising companies.

114. Accordingly, Blue Shield lacked authorization to intercept, disclose to Google, or use Plaintiff's and Class Members' Personal Health Information, or to procure Google to intercept, disclose, or use such Personal Health Information.

G. Plaintiff and Class Members Have a Reasonable Expectation of Privacy in Their Personal Health Information

115. Plaintiff and Class Members have a reasonable expectation of privacy in their personal health information, including personally identifiable data and sensitive medical information. Specifically, Plaintiff and Class Members had a reasonable expectation that their health insurance provider and its associates would not disclose their personal health information to third parties without express authorization.

[32] *Id.*

116. Plaintiff's and Class Members' reasonable expectations of privacy in their personal health information are grounded in, among other things, Blue Shield's status as a health insurance provider, Blue Shield's common law obligation to maintain the confidentiality of members personal health information, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Blue Shield's express and implied promises of confidentiality.

117. It was reasonable for Plaintiff and Class Members to assume that Blue Shield's privacy policies were consistent with Blue Shield's duties to protect the confidentiality of members' personal health information.

118. Indeed, multiple studies examining the collection and disclosure of consumers' sensitive medical information confirm that the disclosure of sensitive medical information violates expectations of privacy that have been established as general social norms.

119. Privacy polls and studies also 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.

120. For example, a recent study by *Consumer Reports* showed that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believed that internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[33]

121. Users act consistently with these preferences. For example, following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to share data when prompted.[34]

---

[33] *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-a3980496907 (last accessed April 15, 2025).

[34] Margaret Taylor, *How Apple screwed Facebook*, WIRED (May 19, 2021), https://www.wired.com/story/apple-ios14-facebook (last accessed April 15, 2025).

122. "Patients are highly sensitive to disclosure of their health information," particularly because it "often involves intimate and personal facts, with a heavy emotional overlay." Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 Rutgers L.J. 617, 621 (2002). Unsurprisingly, empirical evidence demonstrates that "[w]hen asked, the overwhelming majority of Americans express concern about the privacy of their medical records." Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 Berkley Tech L.J. 1523, 1557 (2009).

123. These concerns are not hypothetical. For example, in 2021, the FTC brought charges against Flo Health, a company who, despite its express privacy claims, took control of users' sensitive fertility data and shared it with third parties—a broken promise that, as the FTC described it, "left consumers feeling 'outraged, victimized, and violated.'"[35]

124. The concern about sharing personal medical information is compounded by the reality that advertisers view this type of information as particularly valuable. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one recent article noted, "What is particularly worrying about this process of datafication of children is that companies like [Google] 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."[36]

125. Many privacy law experts have expressed serious concerns about individuals' sensitive medical information being disclosed to third-party companies like Google. As those critics have pointed out, having an individual's personal health information disseminated in ways the individual is unaware of could have serious repercussions, including affecting their ability to obtain life insurance, how much they might pay for such coverage, the rates they might be charged on loans, and the likelihood of their being discriminated against.

[35] Complaint, *In re Flo Health, Inc.* FTC File No. 1923133, Dkt. No. C-4747, https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf (last accessed April 15, 2025).

[36] Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, THE MIT PRESS READER (Jan. 17, 2021), https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth (last accessed April 15, 2025).

126. Blue Shield's surreptitious interception, collection, and disclosure of its members' personal health information to Google therefore violated Plaintiff and Class Member's privacy interests.

H. Plaintiff's Personal Health Information Has Economic Value and Defendant's Unauthorized Disclosure Has Caused Economic Harm

127. It is common knowledge that there is an economic market for consumers' personal data—including the kind of data that Blue Shield has collected and disclosed from Plaintiff and Class Members.

128. In 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals, and that within that context, "age, gender and location information" were being sold for approximately "$0.50 per 1,000 people."[37]

129. In 2015, *TechCrunch* reported that "to obtain a list containing the names of individuals suffering from a particular disease," a market participant would have to spend about "$0.30" per name.[38] That same article noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge" and that the value of a single user's data can vary from $15 to more than $40 per user.[39]

130. Despite the protections afforded by law, there is an active market for health information. Medical information obtained from health providers garners substantial value because of the fact that it is not generally available to third party data marketing companies because of the strict restrictions on disclosure of such information by state laws and provider standards, including the Hippocratic oath. Even with these restrictions, however, a multi-billion-dollar market exists for the sale and purchase of such private medical information.[40]

---

[37] Emily Steel *et al*, *How much is your personal data worth?*, FINANCIAL TIMES (updated Jul. 15, 2017), https://ig.ft.com/how-much-is-your-personal-data-worth (last accessed April 15, 2025).

[38] Pauline Glikman and Nicolas Glady, *What's the Value of Your Data?*, TECHCRUNCH (Oct. 13, 2015), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data (last accessed April 15, 2025).

[39] *Id.*

[40] Aaron Sankin, *Your medical data is for sale, and there's noting you can do about it*, REVEAL NEWS (Jan. 20, 2017), https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-it (last accessed April 15, 2025); *see also* Justin Sherman, *Your Health Data Might Be for Sale*, SLATE (Jun. 20, 2022), *https://slate.com/technology/2022/06/health-data-brokers-privacy.html* (last accessed April 15, 2025).

131. Further demonstrating the financial value of Class Members' medical data, CNBC has reported that hospital executives have received a growing number of bids for user data.[41]

132. Further, individuals can sell or monetize their own data if they so choose. For example, Facebook has offered to pay individuals for their voice recordings,[42] and has paid teenagers and adults up to $20 a month plus referral fees to install an app that allows Facebook to collect data on how individuals use their smart phones.[43] A myriad of other companies and apps such as DataCoup, Nielsen Computer, Killi, and UpVoice also offer consumers money in exchange for access to their personal data.[44]

133. Given the monetary value that data companies like Google have already paid for personal information in the past, Blue Shield has deprived Plaintiff and the Class Members of the economic value of their sensitive medical information by collecting, using, and disclosing that information to Google and other third parties without consideration for Plaintiff and the Class Member's property.

I. Blue Shield is Enriched by Making Unlawful, Unauthorized, and Unnecessary Disclosures of its Patients' Personal Health Information.

134. In exchange for disclosing personal health information about its members, Blue Shield is compensated by Google with enhanced online advertising services, including (but not limited to) retargeting and enhanced analytics functions. The access to these advertising benefits results in enormous financial savings to companies like Defendant because it reduces their advertising costs. Blue Shield has run numerous advertising campaigns on Google, utilizing the advantages it gained by installing Google Tags on its website.

---

[41] Christina Farr, *Hospital execs say they are getting flooded with requests for your health data* (Dec. 18, 2019), CNBC, https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html, CNBC.COM (last accessed April 15, 2025).

[42] Jay Peters, *Facebook will now pay your for your voice recordings*, The Verge (Feb. 20, 2020), https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-prounounciations-app (last accessed April 15, 2025).

[43] Saheli Roy Choudhury and Ryan Browne, *Facebook pays teens to install an app that could collect all kinds of data*, CNBC, https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html (last accessed April 15, 2025).

[44] *See, e.g., Apps that Pay You for Data Collection*, CreditDonkey (June 12, 2021), https://www.creditdonkey.com/best-apps-data-collection.html (last accessed April 15, 2025); *see also Can You Earn Money From Your Data?*, Monetha Blog, https://www.monetha.io/blog/rewards/earn-money-from-your-data last accessed April 15, 2025).

135. Retargeting is a form of online targeted advertising that targets users with ads based on their previous internet actions, which is facilitated through the use of cookies and tracking pixels. Once an individual's data is disclosed and shared with a third-party marketing company, the advertiser is able to show ads to the user elsewhere on the internet.

136. For example, retargeting could allow a web-developer to show advertisements on other websites to customers or potential customers based on the specific communications exchanged by a patient or their activities on a website. Using Google Tags and Google Ads, a website could target ads on Google itself or on the Google advertising network. The same or similar advertising can be accomplished via disclosures to other third-party advertisers and marketers.

137. Once personally identifiable information relating to member communications is disclosed to third parties like Google, Blue Shield loses the ability to control how that information is subsequently disseminated and exploited.

138. The monetization of the data being disclosed by Blue Shield, both by Blue Shield and Google, demonstrates the inherent value of the information being collected.

TOLLING, CONCEALMENT, AND ESTOPPEL

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

140. Blue Shield seamlessly incorporated Google Tags into its websites, providing no indication to users that they were interacting with a website that was closely tracked by Google Analytics and Google Ads.

141. Blue Shield had knowledge that its websites incorporated Google Tags yet failed to disclose that Plaintiff and Class Members' sensitive medical information would be intercepted, collected, used by, and disclosed to Google.

142. Google Tags are purposefully designed and integrated in a way that makes it impossible to identify with the naked eye and its presence can only be discovered through means significantly more sophisticated than possessed by the average internet user.

143. Plaintiff and Class Members could not with due diligence have discovered the full scope of Blue Shield's conduct, because there were no disclosures or other indication that they were interacting with websites employing Google Tags.

144. Further, Plaintiff and Class Members were not on notice to look for Google Tags or integration with Google Analytics or Google Ads, and Blue Shield's overt representations assured them that their personal information was being treated in a confidential manner.

145. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrines of fraudulent concealment and continuing tort. Blue Shield's illegal interception and disclosure of members' personal health information has continued unabated through the date of the filing of Plaintiff's Complaint.

146. Further, Blue Shield was under a duty to disclose the nature and significance of their data collection practices but did not do so. Blue Shield is therefore estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

147. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

148. Plaintiff seeks class certification for the following proposed Class:

> During the fullest period allowed by law, all persons in the United States who are, or were, members of Blue Shield, or any of its affiliates and who exchanged communications at Blue Shield's websites, including https://www.blueshieldca.com, and any other Blue Shield affiliated website, including Blue Shield's member portal.

149. Excluded from the proposed Class are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Blue Shield, Blue Shield's subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Blue Shield or their parents have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Blue Shield's counsel.

150. Plaintiff reserves the right to redefine the Class and/or add Subclasses at, or prior to, the class certification stage, in response to discovery or pursuant to instruction by the Court.

151. **Numerosity:** Fed R. Civ. P. 23(a)(1). The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are millions of individuals whose Personal Health Information may have been improperly disclosed to third parties , and the Class is identifiable within Defendant's records.

152. **Commonality and Predominance:** Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to Plaintiff and Class Members which predominate over any questions affecting only individual members. A class action will generate common answers to the questions below, which are apt to drive resolution:

a. Whether the tracking technology used by Blue Shield is designed to send individually identifiable information from Defendant to third parties;

b. Whether Blue Shield intercepted and/or transmitted to third parties the contents of electronic communications between members and Blue Shield without Plaintiff's and Class Members' consent;

c. Whether Blue Shield's transmittal to third parties of the contents of electronic communications between members and Blue Shield occurred contemporaneous to their making;

d. Whether Blue Shield violated Plaintiff's and Class Members' privacy rights;

e. Whether Blue Shield's acts and practices constitute a breach of contract;

f. Whether Blue Shield's acts and practices were intentional;

g. Whether Blue Shield's acts and practices were negligent;

h. Whether Blue Shield profited from disclosures of Plaintiff's and Class Members' personal health information to third parties;

i. Whether Blue Shield profited from disclosures of patient personal health information to third parties including Google;

j. Whether Blue Shield was unjustly enriched;

k. Whether Blue Shield's acts and practices harmed and continue to harm Plaintiff and Class Members and, if so, the extent of that injury;

l. Whether Plaintiff and Class Members are entitled to equitable relief including, but not limited to, injunctive relief, restitution, and disgorgement; and

m. Whether Plaintiff and Class Members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

153. These common questions of law and fact predominate over any questions affecting only the individual Class Members.

154. Blue Shield engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

155. **Typicality:** Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their Personal Health Information compromised as a result of Defendant's incorporation of Google Analytics and Google Ads, due to Defendant's misfeasance. Plaintiff has no interests that are antagonist to, or in conflict with, the interests of other members of the Class. Plaintiff's claims arise out of the same set of facts and conduct as all other Class Members. Plaintiff and all Class Members are members of Blue Shield who used the websites set up by Blue Shield for its members and are victims of Blue Shield's respective unauthorized disclosures to Google. All claims of Plaintiff and Class Members are based on Blue Shield's wrongful conduct and unauthorized disclosures.

156. **Adequacy of Representation:** Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

157. **Superiority:** Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large

number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

CAUSES OF ACTION

COUNT I
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA"), 18 U.S.C. § 2511(1) *et seq*.
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of Plaintiff and the Class)

158. Plaintiff realleges and incorporates by reference paragraphs 1-157 as if fully set forth herein.

159. Plaintiff brings this claim on behalf of himselfs and all members of the Class.

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

161. 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.

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

163. **Electronic Communications**. The transmission of Personal Health Information between Plaintiff and Class Members and Defendant via its Website 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 photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

164. **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). The contents of Plaintiff's and Class Members' communications include, but are not limited to, IP addresses, Google ID tags, URLs, file downloads,

and the text of search queries, all of which concern substance and meaning of Plaintiff's and Class Members' personal identities and protected health information such as medical conditions, prescriptions, and treatment.

165. **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). Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the source code it embedded and ran on its web properties, contemporaneously and intentionally acquired and redirected the contents of Plaintiff's and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, i.e. Google.

166. **Electronic, 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. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendant's web-servers; and

d. The Google Analytics and Google Ads code deployed by Defendant to effectuate the sending and acquisition of patient communications.

167. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the Google Analytics and Google Ads embedded and operating on its Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiff's and Class Members' electronic communications, for purposes other than providing health insurance services to Plaintiff and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

168. 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).

169. 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).

170. Defendant intentionally used the intercepted communications to increase its profit margins. Defendant specifically used Google Analytics to track and utilize Plaintiff's and Class Members' Personal Health Information for financial gain.

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

172. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via Google Analytics and/or Google Ads.

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

174. 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).

175. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

176. Defendant is a "party to the communication" with respect to member communications. However, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Personal Health Information does not qualify for the party exemption.

177. Defendant's acquisition of a member's communications that were used and disclosed to Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and California, including:

a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;

i. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person … without authorization" from the patient.

ii. 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.

iii. 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

iv. Disclosed individually identifiable health information to Google without patient authorization.

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

b. Common-law invasion of privacy;

c. Violation of California Constitution, Art. I § 1 – Invasion of Privacy; and

d. Violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630, *et seq*.

178. 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 individually-identifiable health information on its Website, because it used its participation in these communications to improperly share Plaintiff's and Class Members' individually-identifiable health information with Google, third-parties that did not participate in these communications, that Plaintiff and Class Members did not know were receiving their individually-identifiable health information, and that Plaintiff and Class Members did not consent to receive this information.

179. Defendant accessed, obtained, and disclosed Plaintiff's and Class Members' Personal Health Information for the purpose of committing the crimes and torts described herein because it would not have been able to obtain the information or the marketing services if it had complied with the law.

180. As such, Defendants cannot viably claim any exception to ECPA liability.

181. 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 has intruded upon, intercepted, transmitted, shared, and used their individually-identifiable health information (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) 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 Class Members' individually-identifiable patient health information without providing any value or benefit to Plaintiff or the Class Members;

c. Defendant received substantial, quantifiable value from its use of Plaintiff's and Class Members' individually-identifiable health information, such as understanding how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiff or the Class Members;

d. Defendant has failed to provide Plaintiff and the Class Members with the full value of the health insurance services for which they paid, which included a duty to maintain the confidentiality of their 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 medical conditions and treatments that Plaintiff and Class Members intended to remain private no longer private.

182. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members 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 II
BREACH OF CONTRACT
(On Behalf of Plaintiff and the Class)

183. Plaintiff realleges and incorporates by reference paragraphs 1-182 as if fully set forth herein.

184. Plaintiff brings this claim on behalf of himself and all members of the Class.

185. Plaintiff and Class Members entered into express contracts with Defendant for the provision of health insurance and access to resources and services provided through Defendant's Website.

186. The Notice of Privacy Practices on Defendant's Website is incorporated into the contract between Blue Shield and its Website users.

187. In its Notice of Privacy Practices, Blue Shield promises that "[o]ther than for [purposes expressly described], we must obtain your written authorization to use or disclose your PHI. For example, we will not use your PHI for marketing purposes without your prior written authorization."

188. Defendant thus undertook an express contractual obligation to obtain prior written authorization from Plaintiff and Class Members before disclosing their PHI for marketing purposes, or indeed for any purpose not expressly described in the Notice of Privacy Practices.

189. Defendant's contractual promise not to disclose PHI to third parties is also evident through the parties' course of conduct.

190. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of health insurance, which included an implied agreement for Defendant to retain and protect the privacy of Plaintiff's and Class Members' Personal Health Information.

191. Defendant solicited and invited Plaintiff and Class Members to provide their Personal Health Information on its website as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Personal Health Information, which included personally identifiable information such as their names, telephone numbers, IP addresses, Google IDs,

browser fingerprints, and device identifiers to Defendant as part of acquiring Defendant's medical services and using its website and patient portal. Per its contractual, legal, ethical, and fiduciary duties, Defendant was obligated to take adequate measures to protect Plaintiff's and Class Members' Personal Health Information from unauthorized disclosure to third parties such as and Google. These facts give rise to the inference that Defendant took on obligations apart from the plain terms of any express contracts that they may have had with Plaintiff and Class Members.

192. Defendant required and obtained Plaintiff's and Class Members' Personal Health Information as part of the contractual relationship, evincing an implicit promise by Defendant to act reasonably to protect the confidentiality of Plaintiff's and Class Members' Personal Health Information. Defendant, through its privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised that it would safeguard Plaintiff's and Class Members' Personal Health Information in exchange for access to that information and the opportunity to provide Plaintiff and Class Members with health insurance.

193. Implied in the exchange was a promise by Defendant to ensure that the Personal Health Information of Plaintiff and Class Members in its possession would only be used for medical treatment purposes and would not be shared with third parties such as Google without the knowledge or consent of Plaintiff and Class Members. By asking for and obtaining Plaintiff's and Class Members' Personal Health Information, Defendant assented to protecting the confidentiality of that information. Defendant's implicit agreement to safeguard the confidentiality of Plaintiff's and Class Members' Personal Health Information was necessary to effectuate the contract between the parties.

194. Plaintiff and Class Members provided their Personal Health Information in reliance on Defendant's implied promise that this information would not be shared with third parties without their consent.

195. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Class Members would provide their Personal Health Information in exchange for the medical treatment and other benefits provided by Defendant (including the protection of their confidential personal and medical information). A portion of the price of each payment that Plaintiff

and the Class Members made to Defendant for medical services was intended to ensure the confidentiality of their Personal Health Information.

196. By express contractual terms and by the parties' course of conduct and reasonable expectations, Defendant was therefore required to safeguard and protect the Personal Health Information of Plaintiff and Class Members from unauthorized disclosure and/or use by third parties.

197. Plaintiff and Class Members accepted Defendant's offer and fully performed their obligations under the contract with Defendant by providing their Personal Health Information to Defendant among other obligations. Plaintiff and Class Members would not have provided and entrusted their Personal Health Information to Defendant in the absence of their contracts with Defendant and would have instead retained the opportunity to control their Personal Health Information for uses other than the benefits offered by Defendant.

198. Plaintiff and Class Members relied on Defendant's contractual promises to safeguard their Personal Health Information to their detriment. Defendant breached the contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff's and Class Members' Personal Health Information from disclosure to Google.

199. Defendant's failure to implement adequate measures to protect the Personal Health Information of Plaintiff and Class Members and Defendant's intentional disclosure of the same to third parties violated the purpose of the agreement between the parties: Plaintiff's and Class Members' provision of money and Personal Health Information in exchange for health insurance and other benefits.

200. Instead of safeguarding Plaintiff's and Class Members' Personal Health Information, Defendant intentionally shared that information with third parties—thereby breaching the contracts it had with Plaintiff and Class Members.

201. Plaintiff and Class Members—who paid money to Defendant—reasonably believed and expected that Defendant would use part of those funds to operate its Website free of surreptitious collection and exploitation of communications between the parties. Defendant failed to do so. Plaintiff and Class Members would not have purchased health insurance from Defendant if they knew that Defendant would share their Personal Health Information with third parties without their knowledge or written consent.

202. Both the provision of health insurance services and the protection of Plaintiff and Class Members' Personal Health Information were material aspects of these implied contracts.

203. Defendant materially breached its contractual obligation to protect the nonpublic Personal Health Information Defendant gathered when it allowed third parties to collect and exploit that information without Plaintiff's and Class Members' consent.

204. Defendant also materially breached its contractual obligation to protect Plaintiff's and Class Members' non-public Personal Health Information when it failed to implement adequate security measures and policies to protect the confidentiality of that information. For example, on information and belief, Defendant:

a. failed to implement internal policies and procedures prohibiting the disclosure of members' Personal Health Information without consent to Google;

b. failed to implement adequate reviews of the source code and java script installed on its websites to ensure that members' Personal Health Information was not being automatically routed without consent to Google;

c. failed to provide adequate notice to the public that visitors to its websites risked having their Personal Health Information shared with Google;

d. failed to take other industry standard privacy protection measures such as providing a "cookie" acceptance button on its website homepages;

e. failed to provide visitors to its websites with a means to opt out of the automatic transfer of data regarding their website interactions to Google;

f. failed to implement internal policies and educational programs to ensure that Defendant's website managers and coders were familiar with the legal regulations governing the disclosure patient Personal Health Information to third parties; and

g. failed to install adequate firewalls or take similar measures to prevent the automatic routing of patients' Personal Health Information to Google.

205. As a result of Defendant's failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains, and instead received health insurance and other services that were of a diminished value compared to those described

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

206. As a result of Defendant's material breaches, Plaintiff and Class Members were deprived of the benefit of their bargain with Defendant because they spent more on products and services with Defendant than they would have if they had known that Defendant was not providing the reasonable data security and confidentiality of their communications that Defendant represented that it was providing in its privacy policies. Defendant's failure to honor its promises that it would protect the confidentiality of patient communications thus resulted in Plaintiff and Class Members overpaying Defendant for the services they received.

207. The products and services that Defendant offers are available from many other health care systems who do protect the confidentiality of patient communications. Had Defendant disclosed that it would allow third parties to secretly collect Plaintiff's and Class Members' Personal Health Information without consent, neither Plaintiff, the Class Members, nor any reasonable person would have purchased health insurance products or other services from Defendant.

208. Defendant's conduct in sharing Plaintiff's and Class Members' Personal Health Information with third parties also diminished the sales value of that information. There is a robust market for the type of information that Plaintiff and Class Members shared with Defendant (which Defendant then disclosed to third parties). For example, Facebook itself has offered to pay the public to acquire similar information in the past so that Facebook could use such information for marketing purposes. Plaintiff and Class Members were harmed both by the dissemination of their Personal Health Information and by losing the sales value of that information.

209. Plaintiff and Class Members would not have retained Defendant to provide health insurance services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

210. Defendant deliberately and consciously breached these contracts by disclosing Plaintiff's and Class Members' Personal Health Information without consent to Google.

211. By deliberately breaching its implied contracts with Plaintiff and Class Members, Defendant was knowingly enriched by the savings in costs that should reasonably have been expended

to protect the Personal Health Information of Plaintiff and Class Members. Defendant was further knowingly enriched by the financial benefits that it received for bartering Plaintiff's and Class Members' Personal Health Information to Google, including analytics and advertising benefits that Defendant received in exchange for Plaintiff's and Class Members' health data.

212. As a direct and proximate result of these failures, Plaintiff and the Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including, without limitation, the release and disclosure of their Personal Health Information, the loss of control of their Personal Health Information, the diminution in value of their Personal Health Information, and the loss of the benefit of the bargain they had struck with Defendant.

213. Plaintiff and Class Members are entitled to compensatory and consequential damages, including attorney's fees and actual damages, as a result of Defendant's breach of implied contract.

214. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT III
Negligence
(On Behalf of Plaintiff and the Class)

215. Plaintiff realleges and incorporates by reference paragraphs 1-214 as if fully set forth herein.

216. Plaintiff brings this claim on behalf of themselves and all members of the Class.

217. Health insurance providers like Defendant owe common law duties to their members to preserve the confidentiality of their Personal Health Information.

218. Separate and independent from any express or implied contractual duties that Defendant owed Plaintiff and the Class Members, Defendant also owed common law duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, safeguarding, deleting, and protecting the Personal Health Information in its possession from being compromised, stolen, accessed, and misused by unauthorized third parties.

219. Defendant's duty to use reasonable care arose from multiple sources. Defendant (1) invited Plaintiff and Class Members to use its Website; (2) retained Plaintiff's and Class Members' Personal Health Information; (3) affirmatively promised Plaintiff and Class Members that it would never

share or sell their Personal Health Information to third parties; (4) was on notice that Personal Health Information could not be freely shared with advertising companies without specific written authorization from patients; (5) was on notice that hackers and other third parties were targeting such information; (6) was on notice that members Personal Health Information has significant monetary value; but (7) failed to implement adequate security and training measures to protect against the foreseeable risk of unauthorized disclosures of Plaintiff's and Class Members' Personal Health Information to third parties like Google.

220. Defendant's affirmative conduct in installing Google tracking technology created the risk that Plaintiff's and Class Members' Personal Health Information could be accessed and misused by unauthorized third parties.

221. Defendant's members including Plaintiff and Class Members, were the foreseeable and probable victims of any inadequate security and privacy practices on the part of Defendant. By collecting and storing Plaintiff's and Class Members' Personal Health Information, Defendant was obligated to act with reasonable care to protect against the foreseeable threat that Plaintiff's and Class Members' Personal Health Information could be accessed, reviewed, and misused by unauthorized third parties. By creating the risk that its patients' Personal Health Information could be accessed by unauthorized third parties, Defendant assumed the duty to act with reasonable care to protect against that risk.

222. Defendant also violated its own internal policies and failed to meet current health care industry data security standards by (1) failing to adequately train its employees regarding their privacy obligations to patients, (2) failing to adequately monitor its marketing employees' use of tracking technologies, (3) failing to provide notice to members that it was sharing their Personal Health Information with third parties, and (4) failing to establish safeguards to ensure compliance with its obligations to protect patient privacy.

223. Defendant knew or should have known that installing tracking technologies such as Google Analytics and Google Ads would create a substantial (indeed, an inevitable) risk that its members' Personal Health Information would be accessed by unauthorized third parties. That is because such tracking technologies are specifically designed to share data with third parties.

224. Defendant also knew or should have known that inadequate electronic data security protections would create a likelihood that its members' Personal Health Information could be compromised and that third parties would avail themselves of the opportunity to access, review, and exploit this sensitive data. The collection and storage of troves of electronic health data stored on internet-accessible servers held by large health insurance companies creates obvious targets for third parties to attempt to access and exploit such data.

225. Defendant knew that it was collecting and storing sensitive Personal Health Information, that any breach of its system would result in an increased risk that members' Personal Health Information would be acquired by unauthorized third parties, that Personal Health Information (which contains both PHI and PII) is extremely valuable, that cyber-attacks and other unauthorized accesses of Personal Health Information are common, and that third parties, including cyber criminals and advertisers, are highly motivated to obtain access to members' Personal Health Information.

226. Defendant breached the duties owed to Plaintiff and Class Members and was thus negligent.

227. For example, Defendant materially breached its common law duties to protect Plaintiff's and Class Members' non-public Personal Health Information against unauthorized disclosures when it failed to implement adequate security measures and policies to protect the confidentiality of that information. For example, on information and belief, Defendant:

a. failed to implement internal policies and procedures prohibiting the disclosure of members' Personal Health Information without consent to Google;

b. failed to implement adequate reviews of the source code and java script installed on its websites to ensure that members' Personal Health Information was not being automatically routed without consent to Google;

c. failed to provide adequate notice to the public that visitors to its websites risked having their Personal Health Information shared with Google;

d. failed to take other industry standard privacy protection measures such as providing a "cookie" acceptance button on its website homepages;

e. failed to provide visitors to its websites with a means to opt out of the automatic transfer of data regarding their website interactions to Google;

f. failed to implement internal policies and educational programs to ensure that Defendant's website managers and coders were familiar with the legal regulations governing the disclosure of members' Personal Health Information to third parties; and

g. failed to install adequate firewalls or take similar measures to prevent the automatic routing of members' Personal Health Information to Google.

228. Defendant also breached the duties owed to Plaintiff and Class Members by, among other things, (a) mismanaging its Website, member portal, and IT system by failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of member information that resulted in the unauthorized access and disclosure of Plaintiff's and Class Members' Personal Health Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect or to report the unauthorized disclosures at the time they began; and (g) failing to follow or to enforce its own privacy policies and practices, including the privacy policies provided to patients.

229. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' Personal Health Information would not have been disclosed without authorization to third parties.

230. As a direct and proximate cause of Defendant's breach of its duties to Plaintiff and Class Members, Plaintiff and Class Members were damaged by Defendant's breach in, at minimum, the following ways:

a. The unauthorized disclosure of their Personal Health Information to multiple third parties;

b. Sensitive and confidential information that Plaintiff and Class Members intended to remain confidential is no longer private;

c. Plaintiff and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertising;

d. Defendant took something of value from Plaintiff and Class Members are derived benefit therefrom without Plaintiff's and Class Members' knowledge or consent and without compensation for their Personal Health Information;

e. Costs associated with detection and prevention of unauthorized use of Plaintiff's and Class Members' medical information;

f. Costs associated with time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the unauthorized disclosure of their medical information;

g. Continued risk of the unauthorized distribution of Plaintiff's and Class Members' Personal Health Information;

h. Forcing Plaintiff and Class Members to live with the perpetual, well-founded fear that Google will misuse their Personal Health Information;

i. Continued substantial risk of becoming victims of identify theft crimes, fraud, and abuse;

j. Loss of Plaintiff's privacy and confidentiality of their Personal Health Information;

k. Defendant's actions diminished the value of Plaintiff's and Class Members' Personal Health Information;

l. Defendant's actions violated the property rights that Plaintiff and Class Members have in their personal information;

m. General damages for invasion of their rights in an amount to be determined at trial; and

n. Nominal damages for each independent violation.

231. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

232. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

233. Plaintiff realleges and incorporates by reference paragraphs 1-232 as if fully set forth herein.

234. Plaintiffs bring this claim on behalf of himself and all members of the Class.

235. Plaintiff bring this claim in the alternative to his claim for breach of contract.

236. Plaintiff and Class Members conferred a benefit on Blue Shield in the form of valuable sensitive medical information that Blue Shield collected from Plaintiff and Class Members under the guise of keeping this information private, and Blue Shield appreciated this benefit. Plaintiffs also conferred a monetary benefit to Defendant in the form of premiums that they paid in premiums for health insurance services.

237. Blue Shield gained access to the Personal Health Information provided by Plaintiff and Class Members by (1) knowingly concealing its use of Google tracking technologies from the public; (2) misrepresenting to the public in its privacy policies about protecting personally identifying information disclosed via the website from unauthorized disclosure to third parties; (3) failing to institute warnings on its website home page that it had installed Google tracking technologies; (4) failing to provide industry standard privacy safeguards for its members' health information; (5) intentionally disregarding years of warnings from the United States Department of Health and Human Services that it was obligated to protect its members' Personal Health Information from unauthorized disclosures to third parties; (6) intentionally violating its own internal privacy policies by making unauthorized disclosures of members' Personal Health Information; and (7) intentionally violating both state and federal law, including HIPAA.

238. Defendant benefitted from the use of Plaintiff's and Class Members' Private Information and the payment of health insurance premiums ,and unjustly retained those benefits at their expense.

239. Defendant collected, used, and disclosed this members' information for its own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Specifically,

Blue Shield bartered Plaintiff's and Class Members' Personal Health Information to Google in return for both advertising benefits and "free" website analytics information. By sharing its members Personal Health Information with Google, Blue Shield gained the ability to utilize Google's targeted advertising features, which saved Blue Shield substantial revenues by making advertising far less expensive than it would have been otherwise. Blue Shield also gained access to free website analytics data, which it otherwise would have had to spend substantial amounts of money to provide for itself.

240. Blue Shield unjustly retained the monies that Plaintiff and Class Members paid with the expectation that Blue Shield would spend a percentage of those funds to implement adequate data security and privacy training to protect their Personal Health Information against unauthorized disclosure to third parties.

241. Plaintiff and the Class Members would not have used Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to third parties like Google.

242. Defendant exceeded any authorization given and instead consciously disclosed and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

243. Google provides Blue Shield with "free" analytics benefits only because the member health data that Blue Shield surreptitiously shared with has an economic value many times in excess of the analytics services that Google provided Blue Shield.

244. Blue Shield wrongfully secured the benefits it obtained from Plaintiff and Class Members by intentionally misleading them about how it would use and exploit their Personal Health Information.

245. Blue Shield unjustly retained those benefits at the expense of Plaintiff and Class Members because Blue Shield's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

246. Plaintiff were aware of the economic value of their Personal Health Information and reasonably expected to be *substantially* compensated by any party who shared or accessed their Personal Health Information to sell advertising. Plaintiff and Class Members did not consent to Defendant giving their health information away for free.

247. Blue Shield unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

248. The benefits that Blue Shield derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members. It would be inequitable and unjust for Blue Shield to be permitted to retain any of the profits or other benefits Defendant derived from the wrongful collection and disclosure of Plaintiff's and Class Members' Personal Health Information as alleged in this

249. Blue Shield should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Blue Shield received, and such other relief as the Court may deem just and proper.

COUNT V
Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class)

250. Plaintiff realleges and incorporates by reference paragraphs 1-249 as if fully set forth herein.

251. Plaintiff brings this claim on behalf of himself and on behalf of the Class.

252. California common law recognizes a cause of action for intrusion upon seclusion.

253. The Personal Health Information of Plaintiff and Class Members consists of private and confidential facts and information that were never intended to be shared beyond private communications.

254. Plaintiff and Class Members had a reasonable expectation of privacy in their sensitive health information.

255. Blue Shield intentionally intruded upon Plaintiff and Class Members' private life, solitude, or seclusion by intercepting the contents of their communications with Blue Shield's Website and disclosing those communications to Google.

256. Plaintiff and Class Members did not consent to, authorize, or know about Blue Shield's intrusion at the time it occurred. Plaintiff and Class Members never agreed that Blue Shield could disclose their sensitive health information to third parties, including Google. Plaintiff intended their

sensitive health information to stay private from third parties without their consent and Blue Shield represented that their sensitive health information would stay private and confidential.

257. Plaintiff and Class Members had an interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

258. Blue Shield's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy because Plaintiff's and Class Members' sensitive health information is private and was intended to remain private and confidential.

259. Plaintiff and Class members were harmed by Blue Shield's wrongful conduct as Blue Shield's conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their sensitive health information.

260. As a direct and proximate result of Blue Shield's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT VI
Violation of California Constitution, Art. I § 1 – Invasion of Privacy
(On behalf of Plaintiff and the Class)

261. Plaintiff realleges and incorporates by reference paragraphs 1-260 as if fully set forth herein.

262. Plaintiff brings this claim on behalf of himself and on behalf of the Class.

263. Article I, Section 1 of the California Constitution states "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

264. Plaintiff and Class Members had, and continue to have, a legally protected interest in their sensitive medical and personal information that they provided Blue Shield, deriving from common law and state and federal statutes, including, *inter alia*, HIPAA, The California Invasion of Privacy Act, and The Confidentiality of Medical Information Act.

265. Plaintiff and members of the Class had a reasonable expectation of privacy in their sensitive medical information and personal data shared Blue Shield, because Plaintiff and members of the Class did not consent to Blue Shield sharing such information with Google.

266. Blue Shield, in violation of its own Privacy Policy, intentionally collected and shared Plaintiff's and Class Members' sensitive medical and personal information without their consent.

267. Blue Shield's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy because Plaintiff's and Class Member's sensitive health information is private and was intended to remain private and confidential.

268. Plaintiff and Class Members were harmed by Blue Shield's wrongful conduct, which has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their sensitive health information.

269. As a direct and proximate result of Blue Shield's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT VII
Violation of the California Invasion of Privacy Act ("CIPA")
Cal. Penal Code §§ 630, et seq.
(on Behalf of Plaintiff and the Class)

270. Plaintiff realleges and incorporates by reference paragraphs 1-269 as if fully set forth herein. Plaintiff brings this claim on behalf of himself and on behalf of the Class.

271. To establish liability under Section 631(a) of the CIPA, a plaintiff must establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner" either (1) "[i]ntentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;" (2) "[w]illfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;" (3) "[u]ses, or attempts to use, in any manner, or for any

purpose, or to communicate in any way, any information so obtained;" or (4) "[a]ids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section."

272. Section 631(a) applies to internet communications and thus applies to Plaintiff's and the Class's sensitive health information which was shared by Blue Shield through Google Tags. *See Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) (citing Cal. Penal Code § 631(a) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications. It makes liable anyone who 'reads, or attempts to read, or to learn the contents' of a communication 'without the consent of all parties to the communication.'"); *In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 608 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

273. Blue Shield's use of Google Tags, to power Google Analytics and Google Ads, is a "machine, instrument, contrivance, or . . . other manner" used to engaged in the prohibited conduct at issue here.

274. Blue Shield procured Google to automatically and secretly spy on, and intercept its patients' sensitive health information communicated through Blue Shield's Website in real time. To facilitate this wiretap, Blue Shield installed Google Tags on its Website and all subpages of its Website.

275. By installing Google Tags on its Website and subpages of its Website, Blue Shield (1) intentionally caused Plaintiff's and Class Members' sensitive health and personal information to be intercepted, recorded, stored, and transmitted to Google and (2) intentionally caused the contents Plaintiff's and Class members' sensitive health and personal information to be accessed by Google.

276. Interception of Plaintiff's and Class Members' private and confidential electronic communications without their consent occurs whenever users engage with any subpage on the Blue Shield Website.

277. Plaintiff and the Class members had a justified expectation under the circumstances that their electronic communications would not be intercepted, especially where Blue Shield is a HIPAA covered entity to whom patients entrust their sensitive health information in order to access resources and services from the Blue Shield Website.

278. Blue Shield had no right to intercept, collect, and disclose the Plaintiff's and the Class Members' sensitive health information. Neither Plaintiff nor the Class consented to Blue Shield's interception, disclosure, and/or use of their sensitive health information in their electronic communications with the Blue Shield Website. Nor could they. Blue Shield never sought to or did obtain Plaintiff's or the Class Members' consent.

279. Blue Shield's conduct has needlessly harmed Plaintiff and the Class by disclosing intimately personal facts and data in the form of their sensitive health information. This disclosure and loss of privacy and confidentiality has caused the Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

280. Plaintiff and Class members seek all relief available relief under Cal. Penal Code § 631, including statutory damages of $2,500 per violation.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, asks for judgment in their favor, and that the Court enter an order as follows:

A. Certifying the Class and appointing Plaintiff as the Class's representative;

B. Appointing Plaintiff's counsel as class counsel;

C. Finding that Blue Shield's conduct as alleged herein was unlawful;

D. Awarding such injunctive and other equitable relief as the Court deems just and proper, including enjoining Blue Shield from making any further disclosure of Plaintiff or Class Members' communications to third parties without the Plaintiff or Class Members' express, informed, and written consent;

E. Awarding statutory damages to Plaintiff and Class Members pursuant to 18 U.S.C. § 2520 and Cal. Penal Code § 631;

F. Imposing a constructive trust against Blue Shield through which Plaintiff and Class Members can be compensated for any unjust enrichment gained by Blue Shield;

G. Awarding damages for violations of Plaintiff and Class Members' right to privacy;

H. Awarding Plaintiff and Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

I. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law;

J. Awarding Plaintiff and Class Members reasonable attorney's fees, costs, and expenses;

K. Awarding costs of suit; and

L. Such other and further relief to which Plaintiff and Class Members may be entitled.

Dated: April 22, 2025

LYNCH CARPENTER, LLP

By: */s/ (Eddie) Jae K. Kim*

(Eddie) Jae K. Kim (SBN 236805)
ekim@lcllp.com
Tiffine E. Malamphy (SBN 312239)
tiffine@lcllp.com
117 E Colorado Blvd, Ste 600
Pasadena, CA 91105-3712
Tel.: (213) 723-0707
Fax: (858) 313-1850

Attorneys for Plaintiff
and Proposed Class Counsel

CIVIL COVER SHEET

This civil cover sheet does not replace or supplement the filing and service of pleadings or other papers. The information on 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. Instructions are on the reverse of this form.

I. PLAINTIFF(S)

AUSTIN KAHN, on behalf of himself and all others similarly situated,

County of Residence of First Listed Plaintiff: Los Angeles
Leave blank in cases where United States is plaintiff.

Attorney or Pro Se Litigant Information *(Firm Name, Address, and Telephone Number)*

LYNCH CARPENTER, LLP, 117 E Colorado Blvd, Ste 600, Pasadena, CA 91105-3712
(213) 723-0707

DEFENDANT(S)

CALIFORNIA PHYSICIANS' SERVICE, D/B/A BLUE SHIELD OF CALIFORNIA,

County of Residence of First Listed Defendant:
Use ONLY in cases where United States is plaintiff.

Defendant's Attorney's Name and Contact Information *(if known)*

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

- ☐ U.S. Government Plaintiff
- ☐ Federal Question *(U.S. Government Not a Party)*
- ☐ U.S. Government Defendant
- ☒ Diversity

III. CAUSE OF ACTION

Cite the U.S. Statute under which you are filing: *(Use jurisdictional statutes only for diversity)*
U.S.C. § 1332(d)

Brief description of case: Unlawful disclosure of confidential Personal Health Information

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 & Enforcement of Judgment
- ☐ 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 U.S.C. § 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)*

- ☒ Original Proceeding
- ☐ Removed from State Court
- ☐ Remanded from Appellate Court
- ☐ Reinstated or Reopened
- ☐ Transferred from Another District
- ☐ Multidistrict Litigation–Transfer
- ☐ Multidistrict Litigation–Direct File

VI. FOR DIVERSITY CASES ONLY: CITIZENSHIP OF PRINCIPAL PARTIES

(Place an "X" in One Box for Plaintiff and One Box for Defendant)

Plaintiff	Defendant	
☒	☒	Citizen of California
☐	☐	Citizen of Another State
☐	☐	Citizen or Subject of a Foreign Country
☐	☐	Incorporated or Principal Place of Business In California
☐	☐	Incorporated and Principal Place of Business In Another State
☐	☐	Foreign Nation

VII. REQUESTED IN COMPLAINT

- ☑ Check if the complaint contains a **jury demand.**
- ☐ Check if the complaint contains a **monetary demand**. Amount:
- ☑ Check if the complaint seeks **class action** status under Fed. R. Civ. P. 23.
- ☐ Check if the complaint seeks a **nationwide injunction** or Administrative Procedure Act vacatur.

VIII. RELATED CASE(S) OR MDL CASE

Provide case name(s), number(s), and presiding judge(s).

IX. DIVISIONAL ASSIGNMENT pursuant to Civil Local Rule 3-2

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

DATE 04/22/2025 **SIGNATURE OF ATTORNEY OR PRO SE LITIGANT** /s/ (Eddie) Jae K. Kim

COMPLETING THE CIVIL COVER SHEET

Complete the form as follows:

I. Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use 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.

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. In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.

Attorney/Pro Se Litigant Information. Enter the firm name, address, telephone number, and email for attorney of record or pro se litigant. If there are several individuals, list them on an attachment.

II. Jurisdiction. Under Federal Rule of Civil Procedure 8(a), pleadings must establish the basis of jurisdiction. If multiple bases for jurisdiction apply, prioritize them in the order listed:

(1) *United States plaintiff*. Jurisdiction based on 28 U.S.C. §§ 1345 and 1348 for suits filed by the United States, its agencies or officers.

(2) *United States defendant.* Applies when the United States, its agencies, or officers are defendants.

(3) *Federal question*. Select this option when jurisdiction is based on 28 U.S.C. § 1331 for cases involving the U.S. Constitution, its amendments, federal laws, or treaties (but use choices 1 or 2 if the United States is a party).

(4) *Diversity of citizenship.* Select this option when jurisdiction is based on 28 U.S.C. § 1332 for cases between citizens of different states and complete Section VI to specify the parties' citizenship. Note: Federal question jurisdiction takes precedence over diversity jurisdiction.

III. Cause of Action. Enter the statute directly related to the cause of action and give a brief description of the cause. Do not cite jurisdictional statutes unless jurisdiction is based on diversity. Example: U.S. Civil Statute: 47 U.S.C. § 553. Brief Description: Unauthorized reception of cable service.

IV. Nature of Suit. Check one of the boxes. If the case fits more than one nature of suit, select the most definitive or predominant.

V. Origin. Check one of the 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 U.S.C. § 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, using 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*. Check this box for cases transferred under Title 28 U.S.C. § 1404(a). Do not use this for within-district transfers or multidistrict litigation (MDL) transfers.

(6) *Multidistrict Litigation Transfer*. Check this box when a multidistrict (MDL) case is transferred into the district under authority of Title 28 U.S.C. § 1407.

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

VI. Residence (citizenship) of Principal Parties. Mark for each principal party *only* if jurisdiction is based on diversity of citizenship.

VII. Requested in Complaint.

(1) *Jury demand.* Check this box if plaintiff's complaint demanded a jury trial.

(2) *Monetary demand*. For cases demanding monetary relief, check this box and enter the actual dollar amount being demanded.

(3) *Class action.* Check this box if plaintiff is filing a class action under Federal Rule of Civil Procedure 23.

(4) *Nationwide injunction.* Check this box if plaintiff is seeking a nationwide injunction or nationwide vacatur pursuant to the Administrative Procedures Act.

VIII. Related Cases. If there are related pending case(s), provide the case name(s) and number(s) and the name(s) of the presiding judge(s). If a short-form MDL complaint is being filed, furnish the MDL case name and number.

IX. Divisional Assignment. 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." Note that case assignment is made without regard for division in the following case types: Property Rights (Patent, Trademark and Copyright), Prisoner Petitions, Securities Class Actions, Anti-Trust, Bankruptcy, Social Security, and Tax.