ISRAEL DAVID*
ISRAEL DAVID LLC
17 State Street, Suite 4010
New York, NY 10004
Tel: 212.739.0622
Email: israel.david@davidllc.com

* *Pro Hac Vice Admission Pending*

Attorneys for Plaintiff Y.W.

MARIO A. MOYA (State Bar No. 262059)
REBECCA M. HOBERG (State Bar No. 224086)
MOYA LAW FIRM
1300 Clay Street, Suite 600
Oakland, California 94612
Tel: 510.926.6521
Fax: 510.340.9055
Email: mmoya@moyalawfirm.com
rhoberg@moyalawfirm.com

Attorneys for Plaintiff Y.W. (Local Counsel)

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

Y.W., 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 DEMAND FOR JURY TRIAL

Plaintiff Y.W. ("Plaintiff") brings this class action complaint (the "Action") on behalf of himself and all others similarly situated against Defendant California Physicians' Service d/b/a Blue Shield of California ("Defendant" or "BS-CA") upon personal knowledge as to himself and his own actions, upon information and belief and upon the investigation of counsel, seeking actual damages, statutory damages, restitution, disgorgement of profit into a constructive trust, pre- and post-judgment interest, reasonable costs and attorneys' fees, injunctive relief and any other relief this Court deems just and proper, as follows:

I. INTRODUCTION

1. Plaintiff brings this action to remedy the secret interception of the contents of highly sensitive communications between healthcare consumers and Defendant, Blue Shield of California, including those consumers' individually identifiable health information and protected health information ("PHI") (referred to collectively as "Private Information" or "PII"). Specifically, BS-CA aided in the interception of communications between Plaintiff and other Class members (defined below) and a website maintained by BS-CA (the "BS-CA Website"). BS CA assisted in the interception of these communications by Google.

2. Plaintiff's and Class Members' electronic communications with BS-CA were secretly and contemporaneously intercepted, recorded, and transmitted to Google without their knowledge or consent whenever they visited any page of the BS-CA Website, including purportedly secure areas that a user needs to "log in" to the BS-CA Website to access.

3. BS-CA actively aided the secret interceptions of healthcare consumers' communications with their website by injecting hidden code into the website. During the loading of webpages on the BS-CA Website, BS-CA assisted Google to intercept communications surreptitiously. The communications were intercepted through tracking technologies hidden on many webpages of the BS-CA Website that permitted Google to

intercept Private Information, including, without limitation, requests for information on particular conditions and treatments, keyword searches, doctor searches, and access to the website's policyholder portal. Those interceptions enabled Google to know that a specific policyholder and patient sought confidential medical care and permitted Google to know about the nature of that medical care. That recipient, in turn, sells Plaintiff's and Class Members' Private Information to marketers who target Plaintiff and Class Members with online advertisements based on communications obtained via tracking technologies.

4. BS-CA did not disclose to healthcare consumers that it helps third parties such as Google, to intercept the contents of their individual communications with the BS-CA Website, nor did BS-CA seek or obtain their consent for such interception. Unlike other websites, for example, the BS-CA did not alert website users upon accessing the website that their communications are being intercepted, either through a pop-up notification or other prominent notification. Instead, during the proposed class period, BS-CA's disclosures were themselves hidden on the website. Even if a user actively searched for and found BS-CA's purported disclosure on how it collected and shared data, BS-CA told healthcare consumers that they did not share the contents of any individual communications in these circumstances.

5. Despite the confidentiality that healthcare consumers expect with respect to their medical conditions and care, BS-CA chose to put its business interests over the privacy of its patients. The unilateral disclosure of users' Private Information in this manner violated the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered § of 42 U.S.C.S.), among other statutory and common laws.

6. As described more fully below, Plaintiff and Class Members have suffered injury as a result of BS-CA's conduct. These injuries include (i) invasion of privacy; (ii) unwanted

targeted advertisements; (iii) loss of the benefit of the bargain; (iv) diminution of value of the disclosed Private Information; (v) statutory damages; (vi) unjust enrichment; and (vii) the continued and ongoing further disclosure of their Private Information.

7. The federal wiretap act, known as the Electronic Communications Privacy Act ("ECPA") (18 U.S.C. § 2511(1), et seq.) prohibits the interception of the content of any electronic communication. Although the ECPA is often described as a one-party consent wiretap statute, the ECPA's prohibitions apply even when one of the parties to the communications knows about the interception if the communication is intercepted for the purpose of committing any criminal or tortious act—that is, in such circumstances, the ECPA becomes a two-party consent statute. Here, BS-CA disclosed the intercepted electronic communications at issue in a manner that violated HIPAA and constituted independent torts and violations of California common law. The ECPA thus provides a private remedy for BS-CA's interception of electronic communications, enforceable against both the intercepting party and any party that aids such an interception.

8. Plaintiff here asserts statutory remedies under the ECPA both on his own behalf and on behalf of all other individuals who accessed the BS-CA Website. Plaintiff also asserts class claims for breach of implied contract, negligence and unjust enrichment.

II. JURISDICTION, VENUE and INTRADISTRICT ASSIGNMENT

9. *Subject Matter Jurisdiction.* This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1331 as this matter raises federal questions under the ECPA.

10. *Personal Jurisdiction.* This Court has personal jurisdiction over Defendant because it is headquartered in this District, Defendant's acts or practices were directed toward this State and District (and thus, Defendant intentionally availed itself of this jurisdiction by choosing to do business here), and Defendant knew or should have known that the tracking

technologies at issue were being used to intercept the actions of Class members in this Action, as its website is used throughout the United States, including here in this District.

11. *Venue.* Venue is proper because the Defendant is located in and conducts business in this District, Defendant's acts or omissions were directed toward this District and, because Class members were harmed here, and a substantial part of the events, acts and omissions giving rise to Class members' claims occurred here.

12. *Intradistrict Assignment.* Pursuant to Civil Local Rule 3-2(c)-(d), this case should be assigned to the San Francisco or Oakland Divisions because a substantial portion of the events or omissions giving rise to the claim occurred in Alameda County, California.

III. PARTIES

Plaintiff Y.W.

13. Plaintiff Y.W. is a resident of the state of Florida.

14. During the relevant period, Plaintiff was a customer and client of Defendant. As a customer and client of Defendant, Plaintiff visited the BS-CA Website on multiple occasions. While on Defendant's website, Plaintiff was entirely unaware that he was being surreptitiously tracked in order to collect Plaintiff's data. Plaintiff was not informed about the interception of his sale of his data by Google, and was not provided any compensation for his sensitive and valuable information.

15. Plaintiff has suffered the following from (1) the interception of his sensitive private and valuable data, (2) the disclosure of his sensitive private and valuable data to unauthorized third parties, and (3) the failure to justly compensate Plaintiff for his sensitive valuable information the following injuries:

a. The loss of value of personally identifiable information and/or protected health information that might be associated with Plaintiff's visits to Defendant's website;

b. Intrusion upon Plaintiff and Class members' privacy in a place or location whereby it was reasonable for Plaintiff and Class members to have an expectation of privacy while on Defendant's website;

c. Lack of compensation for the sale of Plaintiff and Class members' data; and

d. Profiting from the sale of Plaintiff and Class members' data in a way that would be inequitable sans disgorgement of profit;

Defendant Blue Shield of California

16. Defendant is a provider of health insurance coverage to millions of California residents. Defendant's principal place of business is located in Oakland, California.

17. In the course of doing business, Defendant maintains the BS-CA Website. This website is used by consumers, like Plaintiff and Class members, in order to procure information and services from Defendant.

IV. FACTUAL ALLEGATIONS

The Data Breach and Defendant's Business

18. On April 9, 2025, Plaintiff received a notice from Defendant via email (the "Notice"). The Notice stated that, on February 11, 2025, BS-CA discovered that, between April 2021 and January 2024, Google Analytics, which was used on the BS-CA Website, was configured in a manner that allowed certain member information to be shared with Google's advertising product, and that Google may have used this data to conduct focused ad campaigns targeted at Plaintiff.

19. The Notice further stated that the "information that may been impacted includes the following: Insurance plan name, type and group number; city; zip code; gender; family size; Blue Shield assigned identifiers for your online account; medical claim service date and service provider; patient name, and patient financial responsibility; and "Find a Doctor" search criteria and results (location, plan name and type, provider name and type)."

20. By its very nature, Defendant's healthcare insurance business is the type of business that requires heightened (and, indeed, the highest) levels of privacy. Defendant promised discretion both in the way it conducts its business as well as with respect to the data it collects through its website (and through other means).

21. Consumers understood this when they used the BS-CA Website.

22. This is why Defendant makes privacy assurances and representations through its Privacy Policy, which can be found on its website: to reassure consumers that their visits to Defendant's website are protected in addition to the data that those consumers provide. Representations in the Privacy Policy include:

a. "We at Blue Shield respect your privacy and we work hard to protect the information you provide online.";

b. "We do not sell your personal information. Any personal information you provide on our website or App will be used only in ways consistent with this, the HIPAA and the GLBA Privacy Notices, and in accordance with applicable laws and regulations."; and

c. "Please know that third party service providers are authorized to use your personal information only as necessary to provide services to us."

//

Defendant Collects (and Allows for the Collection) and Resale of Private Data

23. Rather than keep this private information, Defendant instead opted to make it available for collection and sale to Google. Defendant either knew (and was likely profiting from) or should have known that third parties such as Google were using its website as a means to collect advertising data. Google used ad trackers in order to collect data on Plaintiff and Class members, then used those surreptitious trackers as a means to serve digital advertisements to Plaintiff and Class members either on various online platforms (like social media platforms) or on other websites spread throughout the internet.

24. Once Google acquires Plaintiff's and Class members' data, it then uses that data for a variety of purposes, including use for advertising (which is the primary purpose) but also for resale to additional downstream third-party purchasers who may have even less upstanding uses for the data collected. This data is highly valuable, and because a variety of different end users could have utilization for it, it maintains its value as it is collected, sold and resold. Defendant allows for the collection of this data at its primary source: directly from Plaintiff and Class members themselves.

25. As such, Defendant either monetized or allowed for the monetization of this valuable data. And here, Defendant collects health related data which has an even higher value than ordinary data. For example, a data aggregator called Datarade.ai advertises access to vast amounts of data tied to individual U.S. citizens, including name, address, email address and telephone number as well as the information that the specific citizen was shopping for a prescription medication. The starting price for access to this data begins at $10,000. Other healthcare companies, like Pfizer, spend millions annually to purchase health data.

26. Here, Defendant used the data collected from its website users to serve personal advertisements – and many of these advertisers would have no way of knowing that a potential

consumer was in the market for their services without the datapoints sold by Defendant. The lifeblood for some of these businesses is their advertising: and the ability afforded to them by Defendant to know who potential consumers are is simply too good to resist – even at the cost of that consumer's privacy.

The Implications of the Secret Collection of Health Data and Resale of that Information

27. Defendant's conduct violates multiple laws as well as basic notions of consumer privacy (especially in the healthcare context).

28. *Defendant's Conduct Violates HIPAA.* The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which was passed in 1996, sets a floor for the care that healthcare providers across the country are expected to provide in handling patient information. Consumers reasonably expect that healthcare providers will handle their private health information in accordance with HIPAA requirements, including by refraining from sharing that information with ad tech companies. Additionally, by receiving ill-gotten private data, especially valuable PII in combination with sensitive PHI, the advertisers each served as a conduit for Defendant to monetize this precious and private information.

29. In December 2022, the United States Department of Health and Human Services ("HHS") issued a revised bulletin "to highlight the obligations" of healthcare providers under the HIPAA Privacy Rule "when using online tracking technologies" such as those used by Defendant, which "collect and analyze information about how internet users are interacting with a regulated entity's website or mobile application." The bulletin was updated in 2024.

30. In the bulletin, HHS confirmed that HIPAA applies to healthcare providers' use of tracking technologies like those used by Defendant on its website. Among other things, HHS explained that healthcare providers violate HIPAA when they use tracking technologies that

disclose an individual's identifying information, even if no treatment information is included and even if the individual does not have a relationship with the healthcare provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> Some regulated entities may be disclosing a variety of information to tracking technology vendors through tracking technologies placed on the regulated entity's website or mobile app, such as information that the individual types or selects when they use the regulated entities' website or mobile apps. The information disclosed might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, device IDs, or any unique identifying code. In some cases, the information disclosed may meet the definition of individually identifiable health information (IIHI), which is a necessary pre-condition for information to meet the definition of PHI when it is transmitted or maintained by a regulated entity.
>
> 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 in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates or types of healthcare services.

31. Additionally, HHS further clarified that HIPAA applies to healthcare providers with tracking technologies even on webpages and on mobile applications that do not require patients to login. This HHS bulletin did not create any new obligations, but instead highlights obligations that have been in place for decades. Reasonable consumers would expect that Defendant would comply with these obligations with regard to information about the purchase made on Defendant's website.

32. *Defendant's Conduct Violates the FTC Act.* Under the FTC Act and relevant jurisprudence, the Federal Trade Commission has the authority to bring lawsuits against defendants who invade and violate consumers' privacy rights.

33. The FTC has brought actions in federal court against corporations who secretly collect health-related data in the same manner as collected here (including but not limited to *United States of America v. GoodRx Holdings, Inc.*) as well as against corporations who aggregate data collected from third parties through the advertising exchange process, similar to

here (including but not limited to *In the Matter of Mobilewalla, Inc.* and *In the Matter of Gravy Analytics, Inc.*). In each of these actions, the FTC has articulated that consumer protection statutes not only exist to redress privacy related harms, but that those same statutes specifically were intended to protect against the same conduct as alleged in this Action.

34. *Defendant's Conduct Offends Basic Privacy Rights.* Individuals dealing with Defendant, as a provider of health insurance coverage, have a reasonable expectation of privacy because of the sensitive nature of the type of business that Defendant operates. This is especially true here, where Plaintiff and Class members did not anticipate, invite or consent to the presence of Google (or other third-parties) looking over their digital shoulders as they transact business with Defendant.

35. The identifying datapoints collected by Defendant (as detailed above) are highly sensitive information. However, rather than protect this information, Defendant allowed it to be collected, retained and used by Google without the consent of Plaintiff and Class members.

The Value of Consumer Health Data

36. Plaintiff and Class members were harmed when Defendant invaded their privacy rights by making their sensitive personal data available for sale. Reasonable consumers, including Plaintiff, would not have used Defendant's website had they known that their privacy rights would be invaded as a result.

37. PII and PHI is extremely valuable. There is a huge market for the data collected on the BS-CA Website. Plaintiff and Class members have suffered pecuniary losses when Defendant sold and allowed for the resale of their data to Google because of the value of the data itself.

38. The value of consumers' PII and PHI is axiomatic. As stated in "Exploring the Economics of Personal Data," "[f]irms are now able to attain significant market valuations by

employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks." Consumer personal information is so valuable to identity thieves that once PII and PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

39. As the health insurance industry continues to grow, so too are the desires of the advertising industry to profit from the data that accompanies demographic and personal information, as well as consumer interest and consumer purchases.

Harm to Consumers

40. Plaintiff and Class members provided their data to Defendant in order to obtain information regarding the healthcare insurance that Defendant provides. This information was disclosed to and intercepted by Google through ad tracking technology. This information was collected and intercepted for business purposes, including to serve targeted advertising.

41. Plaintiff did not consent to the interception or disclosure of this data to these third parties, or to anyone else. As such, Plaintiff has suffered from the type of privacy-centric harms that a patchwork of privacy protections under federal and state law as well as common law principles were intended to protect against.

V. CLASS ACTION ALLEGATIONS

42. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class (the "Class"):

> All natural persons in the United States who used the BS-CA Website and/or mobile application and whose communications and/or data was shared with (or intercepted by) Google and/or other third parties during the applicable statutory period.

43. Excluded from the Class are: (1) any Judge presiding over this action; and (2) Defendant, Defendant's subsidiaries, affiliates, parents, successors, predecessors, and any entity

in which Defendants or its parents have a controlling interest, and their respective current or former officers, and directors.

44. *Numerosity*. The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists of millions of individuals, and the members can be identified through Defendant's records.

45. *Predominant Common Questions*. The Class's claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant violated Plaintiff's and Class members' privacy rights;

b. Whether Defendant was unjustly enriched;

c. Whether Defendant acted negligently;

d. Whether Defendant breached any implied contracts with Plaintiff and the Class;

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

f. Whether Plaintiff and the Class are entitled to actual, statutory, punitive and/or other forms of damages, and other monetary relief.

46. *Typicality*. Plaintiff's claims are typical of the claims of the other members of the claims of Plaintiff and the members of the Class arise from the same conduct by Defendant and are based on the same legal theories.

47. *Adequate Representation*. Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigation to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and

Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor his counsel have any interest adverse to the interests of the other members of the Class.

48. This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

49. Plaintiff may revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

COUNT ONE
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF THE CLASS)

50. Plaintiff re-alleges and incorporates each of the preceding paragraphs with the same force and effect as if fully restated herein.

51. Plaintiff and Class members each respectively entered into an implied contract with Defendant when they accessed Defendant's website and/or mobile application. Specifically, this implied contract is an agreement by Defendant to safeguard information given to it by Plaintiff and Class members: especially PII and PHI. The existence of Defendant's aforementioned express representations regarding online privacy is evidence of the implied contract between Plaintiff and the Class members, on the one hand, and Defendant, on the other.

52. Plaintiff and Class members had a reasonable expectation that Defendant would keep their PII and PHI confidential. Additionally, Plaintiff and Class members believed that Defendant would use part of the money paid to Defendant in order to keep their PII and PHI confidential.

53. Plaintiff and Class members would not have provided nor entrusted Defendant with their PII or PHI, or would have paid less for its services, had they known that Defendant had no intention of keeping this implied contract.

54. As a direct and proximate cause of Defendant's breach of implied contract, Plaintiff and Class members sustained actual losses and damages as described in detail above, including that they did not get the benefit of their bargain for which they paid and were overcharged by Defendant for its services.

55. Plaintiff and Class members request all forms of damages with respect to these breaches of implied contract, including nominal damages.

COUNT TWO
NEGLIGENCE
(ON BEHALF OF THE CLASS)

56. Plaintiff re-alleges and incorporates each of the preceding paragraphs with the same force and effect as if fully restated herein.

57. Plaintiff and Class members provided Defendant with sensitive, nonpublic personal information. This information included both PII and PHI, as discussed above.

58. While Defendant's conduct was intentional as alleged, it was at a minimum (and in the alternative) negligent.

59. By collecting, storing, using and profiting from this data, Defendant owed a duty of care to Plaintiff and Class members to exercise reasonable care in keeping this information confidential.

60. Defendant had common law duties to prevent foreseeable harm to Plaintiff and Class members. These duties existed because Plaintiff and Class members were foreseeable victims of any disclosure of this PII and PHI without the requisite consent.

61. Defendant's duties to protect the confidentiality of Plaintiff's and Class members nonpublic information, including PII and PHI, also arose as a result of the special relationship that existed between Plaintiff and Defendant – here, between patient and healthcare insurance provider. Defendant alone could have ensured that it did not disclose the nonpublic personal information, including PII and PHI without consumers' consent.

62. Defendant knew or should have known that by integrating the tracking technologies on Defendant's website that it was systemically disclosing PII and PHI to third parties.

63. But for Defendant's conduct, Plaintiff's and Class members' PII and PHI would not have been disclosed without consent. As a direct and proximate cause of this conduct, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial.

64. Plaintiff and Class members seek to recover the value of the unauthorized access to their PII and PHI resulting from Defendant's wrongful conduct.

65. Plaintiff and Class members have a protectable property interest in their PII and PHI; the minimum damages value for the unauthorized use of personal property is its rental value; and rental value is established with respect to market value (*i.e.,* evidence regarding the value of similar transactions). Put differently, the value of the data is equivalent to whatever the unauthorized third parties pay for that respective data.

66. As such, Plaintiff seeks damages in an amount to be proven at trial.

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

68. In addition to or alternatively to this count, Plaintiff also pleads a negligence per se count because Defendant's conduct violates HIPAA as well as the FTC Act.

COUNT THREE
UNJUST ENRICHMENT
(ON BEHALF OF THE CLASS)

69. Plaintiff re-alleges and incorporates each of the preceding paragraphs with the same force and effect as if fully restated herein.

70. This cause of action is pled in the alternative to the breach of implied contract cause of action (Count One).

71. Defendant received benefits from Plaintiff and Class members and unjustly retained those benefits at their expense.

72. Defendant received benefits from Plaintiff and Class members in the form of the Plaintiff's highly valuable data, including health information and PII, that Defendant wrongfully disclosed and intercepted from Plaintiff and Class members without authorization and proper compensation.

73. Defendant disclosed, intercepted, stored, and used this data for its own gain, providing Defendant with economic, intangible, and other benefits, including highly valuable data for analytics, advertising, and improvement of their platforms, algorithms, and advertising services.

74. Had Plaintiff and Class members known of Defendant's misconduct, they would not have provided any of their valuable data to Defendant or have used or paid to use the Defendant's website.

75. Defendant unjustly retained these 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.

76. The benefits that Defendant derived from Plaintiff and Class members rightly belong to Plaintiff and Class members. It would be inequitable under unjust enrichment principles for Defendant to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

77. Defendant should be compelled to disgorge profits into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT FOUR
VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2510 *et seq.*
(ON BEHALF OF THE CLASS)

78. Plaintiff re-alleges and incorporates each of the preceding paragraphs with the same force and effect as if fully restated herein.

79. The Electronic Communications Privacy Act ("ECPA") makes it illegal intentionally to intercept, or attempt to intercept, any wire, oral, or electronic communication and to disclose or use the contents of an unlawfully intercepted communication. 18 U.S.C. § 2511.

80. ECPA provides a private right of action to any person whose electronic communications are intercepted. 18 U.S.C. § 2520(a).

81. Defendant intentionally intercepted electronic communications that Plaintiff and the Class members exchanged with Defendant through the tracking tools installed on its website.

82. The transmission of data between Plaintiff and the Class members and Defendant qualify as communications under ECPA. 18 U.S.C. § 2510(12).

83. Defendant contemporaneously intercepted and transmitted Plaintiff's and the Class members' communications of that data to Google, whose trackers Defendant installed or allowed to be installed on its website.

84. The technology that Defendant and/or Google uses to track Plaintiff's and the Class members' communications, Plaintiff's and the Class members' browsers, Plaintiff's and the Class members' computing devices, and the code that Defendant placed or allowed to be placed on its website are all "devices" within the meaning of 18 U.S.C. § 2510(5).

85. Google, as the recipient of communications between Plaintiff and the Class members, on the one hand, and Defendant, on the other, was not party to those communications.

86. Defendant transmits the contents of those communications through the surreptitious redirection of the communications from Plaintiff's and the Class members' computing devices.

87. Plaintiff and the Class members did not consent to Google's acquisition of their communications with Defendant. Nor did Google receive legal authorization to receive such communications.

88. In disclosing the content of Plaintiff's and the Class members' communications with Defendant (and Defendant's website), Defendant had a purpose that was tortious, criminal, and designed to violate statutory, common law, and constitutional privacy provisions including:

a. The unauthorized disclosure of individually identifiable health information is tortious in and of itself, regardless of whether the means deployed to disclose the information violates the ECPA or any subsequent purpose or use. Defendant intentionally committed a tortious act by disclosing individually identifiable health information without authorization to do so;

b. Intrusion upon Plaintiff's and the Class members' seclusion;

c. Trespass upon Plaintiff's and the Class members' personal and private property; and

d. Violation of 18 U.S.C. §§ 1343 (fraud by wire, radio, or television) and 1349 (attempt and conspiracy) which prohibit a person from "devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate … commerce, any writing, signs, signals, pictures, or sounds for purpose of executing such scheme or artifice."

89. The federal wire fraud statute, 18 U.S.C. § 1343, has four elements: (1) that the defendant voluntarily and intentionally devised a scheme to defraud another out of money or property; (2) that the defendant did so with intent to defraud; (3) that it was reasonably foreseeable that interstate wire communications would be used; and (4) that interstate wire communications were used. The attempt version of the statute provides that penalties apply to attempts as well as offenses. 18 U.S.C. § 1349.

90. Defendant's scheme or artifice to defraud consists of the false and misleading statements in its privacy policy described herein.

91. Defendant acted with intent to defraud in that it willfully invaded and took Plaintiff's and the Class members' property, including the property rights to their individually identifiable health information and their right to determine whether such information remains confidential; the right to determine who may collect and use such information for marketing; and the right to determine who has access to their devices and communications.

92. Defendant also acted with intent to defraud in that it willfully invaded and took Plaintiff's and the Class members' property (their PHI and PII) with knowledge that it lacked

consent or authorization to do so; a reasonable consumer would not understand that Defendant was collecting and transmitting their data to third parties; a reasonable consumer would be shocked to realize the extent of Defendant's disclosure of data to third parties; and the subsequent use of health information for marketing was a further invasion in that the use was not related to any healthcare.

93. Defendant acted with the intent to acquire, use, and disclose Plaintiff's and the Class members' PII and PHI without their authorization or consent.

94. Plaintiff and the Class members have suffered damages because of Defendant's violations of ECPA, including that (1) Defendant eroded the essential, confidential nature of the relationship between Defendant and its customers, (2) Defendant failed to provide Plaintiff and the Class members with the full value of the services for which they paid, which included a duty to maintain confidentiality and protect privacy, (3) Defendant derived valuable benefits from using and sharing Plaintiff's and the Class members' communications without their knowledge or informed consent and without providing compensation, (4) Defendant's actions deprived Plaintiff and the Class members of the value of their PII and PHI, (5) Defendant's actions diminished the value of Plaintiff's and the Class members' property rights in their PII and PHI; and (6) Defendant violated Plaintiff's and the Class members' privacy rights by sharing their PII and PHI for commercial use.

95. Plaintiff and the Class members seek appropriate declaratory or equitable relief including injunctive relief, actual damages and profits enjoyed by Defendant as a result of violations or the appropriate statutory measure of damages, punitive damages, and reasonable attorneys' fees and costs. 18 U.S.C. § 2520. Pursuant to 18 U.S.C. § 2520, Plaintiff and the Class members seek monetary damages for the greater of (i) the sum of the actual damages

suffered by the plaintiff and any profits made by Defendant as a result of the violation or (ii) statutory damages of whichever is greater of $100 a day for each violation or $10,000.

96. Unless enjoined, Defendant will continue to commit the violations of law described herein.

VI. DEMAND FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the proposed Class respectfully requests that the Court enter an order:

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

B. Finding that Defendant's conduct was unlawful, as alleged herein;

C. Awarding declaratory relief against Defendant;

D. Awarding such injunctive and other equitable relief as the Court deems just and proper, including injunctive relief;

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

F. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

G. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

H. Granting such other relief as the Court deems just and proper.

VII. JURY TRIAL DEMANDED

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

DATED: April 10, 2025

Respectfully Submitted,

ISRAEL DAVID LLC

*/s/ Israel David**
Israel David*

**Pro Hac Vice Admission Pending*

Attorneys for Plaintiff Y.W.

MOYA LAW FIRM

/s/ Mario A. Moya
Mario A. Moya

Attorneys for Plaintiff Y.W. (Local Counsel)