

1 Hart L. Robinovitch (AZ SBN 020910)
2 **ZIMMERMAN REED LLP**
3 14646 North Kierland Blvd., Suite 145
4 Scottsdale, AZ 85254
5 Telephone: (480) 348-6400
6 Facsimile: (480) 348-6415
7 Email: hart.robinovitch@zimmreed.com

8 David S. Almeida (*pro hac vice forthcoming*)
9 Elena A. Belov (*pro hac vice forthcoming*)
10 **ALMEIDA LAW GROUP LLC**
11 849 W. Webster Avenue
12 Chicago, Illinois 60614
13 Tel: (312) 576-3024
14 david@almeidalawgroup.com
15 elena@almeidalawgroup.com

16 *Attorneys for Plaintiffs & the Classes*

17
18 **IN THE UNITED STATES DISTRICT COURT**
19 **DISTRICT OF ARIZONA**
20

21 Cheryl McCulley, Rebecca Blount, Cindy
22 Freriks, Jill Schreidl, John Schreidl, and
23 Demetria Ann Santiago-Laboy, *individually*
24 *and on behalf of all others similarly situated,*

25 Plaintiffs,

26 v.

27 Banner Health,

28 Defendant.

Case No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Cheryl McCulley, Rebecca Blount, Cindy Freriks, Jill Schreidl, John Schreidl, and Demetria Ann Santiago-Laboy (collectively “Plaintiffs”) bring this class action lawsuit, individually and on behalf of all others similarly situated, against Defendant BANNER HEALTH (“Banner” or “Defendant”) and allege, upon personal knowledge as to their own actions, their counsel’s investigation and upon information and good faith belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Information concerning a person’s physical and mental health is among the most confidential and sensitive information in our society and the mishandling of such information can have serious consequences, including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.¹

2. Simply put, if people do not trust that their sensitive private information will be kept private and secure, they may be less likely to seek medical treatment which can lead to much more serious health consequences down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to any unauthorized entities is vitally necessary to maintain public trust in the healthcare system as a whole.

3. Protected and highly sensitive medical information collected by healthcare entities includes many categories, from intimate details of an individual’s treatment to any unique identifying code which can connect the individual to the collecting entity.

4. Even internet protocol (“IP”) addresses – which in theory could be connected to

¹ 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/> (last visited May 29, 2023) (“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, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *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> (last visited May 29, 2023).

several members of the same household – are considered personal health information *even when the individual does not have an existing relationship with the regulated healthcare entity* since when the medical provider collects this information through its website, it is indicative that the individual has received or will receive health care services or benefits from the medical provider.²

5. This case concerns a very serious breach of Banner’s data privacy and security obligations as it installed certain tracking technologies on its digital properties to collect and to disclose to unauthorized third parties Plaintiffs’ and Class Members’ personally identifiable information (“PII”) and non-public personal health information (“PHI” and with PII, “Private Information”) for its own pecuniary gain.

6. Specifically, in order to gain additional insights into its patients, improve its return on its marketing dollars and, ultimately, to increase its revenue, Banner encouraged Plaintiffs and Class Members to access and to use various digital tools via its digital properties in order to, among other things, receive healthcare services.³

7. Banner is a non-profit health care system that offers hospital care, hospice care, nursing, surgical, laboratory and rehabilitation services. It provides community-based social service programs and health-related educational programs. The organization owns and leases clinics, hospitals, clinical laboratories, nursing homes, home health agencies, and ambulatory surgery centers and manages other healthcare-related companies, including health insurance companies. Banner operates through a network of medical centers, institutes, concussion centers, health centers, health clinics, research institutes, children’s medical centers, laboratories, occupational health centers, senior centers and residences, surgery centers, and urgent care centers. *See* www.bannerhealth.com.

8. Plaintiff Banner Health is an Arizona non-profit corporation with its principal

² HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaaonline-tracking/index.html> (last visited March 18, 2023).

³ *See* <https://account.bannerhealth.com/sign-in> (encouraging patients to sign up for the Banner Health account so that they may “Find doctors, schedule an appointment, pay your bill, and more and more!”) (last visited May 29, 2023).

place of business in Phoenix, Arizona, and is authorized to do and is doing business in Arizona. Banner operates in several states including Arizona, California, Colorado, Nebraska, Nevada and Wyoming.⁴ Banner is not a public entity.

9. Banner Health is one of the largest health care systems in the country, with more than 50,000 employees, 28 hospitals and a growing network of health centers and clinics.⁵

10. Banner owns, maintains and controls a website, www.BannerHealth.com (the “Website”), which it encourages patients to use for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, signing up for events and classes and more.

11. Defendant also maintains a web-based patient Account called Banner Health Account (the “Account”) whereby registered users can access their account to: (i) communicate with their doctors; (ii) access lab and test results; (iii) manage prescriptions and request refills and (iv) manage appointments, among other things.⁶

12. The Website and the Account are referred to herein as the “Web Properties.”

13. Plaintiffs and Class Members who visited and used (collectively, the “Users”) Defendant’s Web Properties understandably thought they were communicating *only* with their trusted healthcare providers.

14. Unfortunately, Banner intentionally chose to put its revenues over the privacy of its Users. Specifically, Banner installed the Meta Pixel and other tracking technologies on its Web Properties in order to intercept and to send Private Information to third parties such as Meta Platforms, Inc. d/b/a Facebook (“Facebook”) and/or Google LLC without the informed consent of its Users. Rather than disclose to Plaintiff and the Class that it installed Meta Pixel and other

⁴ <https://www.bannerhealth.com/-/media/images/project/bh/about/usa-facilities-wstatistics-11117.ashx> (last visited May 29, 2023).

⁵ <https://www.bannerhealth.com/about/glance/history> (last visited May 29, 2023).
https://www.bannerhealth.com/-/media/files/project/bh/about/banner_20thanniversary_forweb.ashx

⁶ <https://account.bannerhealth.com/sign-in;>
<https://www.bannerhealth.com/patients/banner-app> (last visited May 29, 2023).

1 tracking technologies on its Web Properties in order to intercept and to send Private Information
 2 to third parties such as Meta Platforms, Inc. d/b/a Facebook (“Facebook”) and/or Google LLC,
 3 Banner denied that it used them.⁷

4 15. The Private Information illegally sent to these third parties is, in turn, associated
 5 with other information to create very fulsome user profiles that are mined for marketing and
 6 other commercial purposes. For example, in the case of information sent by Banner to Facebook,
 7 such information was then linked to Plaintiffs’ unique Facebook user ID (“Facebook ID” or
 8 “FID”) so that there was no anonymity in that Facebook and/or any third parties who were able
 9 to access the information would be able to associate such personal health data with Plaintiffs
 10 and all class members.

11 16. Banner breached confidentiality and violated Plaintiffs’ (as well as millions of
 12 other users’) privacy when it unilaterally chose to embed the Pixel and other tracking
 13 technologies to share Private Information with third parties.⁸ Any representation by Defendant
 14 in its Banner Health Privacy Statement that it does not use Pixels is false, deceptive and
 15 misleading.⁹

16 17. As detailed herein, Banner owed common law, statutory and regulatory duties to
 17 keep Plaintiffs’ and class members’ communications and medical information safe, secure and
 18 confidential. First, the disclosure of Plaintiffs’ and class members’ Private Information via the

19 _____
 20 ⁷ <https://www.bannerhealth.com/about/legal-notices/privacy>:

21 **Information Collected Using Pixel Tags or Clear GIFs.**

22 Pixel Tags or Clear GIFs, also known as Web Beacons or Web Bugs, are transparent graphical
 images placed on a website. Currently, Banner Health does not use them on its site.

23 (last visited May 25, 2023)

24 ⁸ Molly Osberg & Dhruv Mehrotra, *The Spooky, Loosely Regulated World of Online*
 25 *Therapy*, JEZEBEL (Feb. 19, 2020), available at <https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137> (last visited May 29, 2023); *see also* Timothy
 26 M. Hale, PhD & Joseph C. Kvedar, MD, *Privacy and Security Concerns in Telehealth*, (Dec.
 27 2014), <https://journalofethics.ama-assn.org/article/privacy-and-security-concerns-telehealth/2014-12>, *AMA JOURNAL OF ETHICS* (last visited May 29, 2023) (illustrating that
 problems with privacy and telehealth apps started to surface as early as 2014).

28 ⁹ <https://www.bannerhealth.com/about/legal-notices/privacy> (last visited May 29, 2023).

Pixel contravenes 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 Private Information.

18. While healthcare organizations regulated under HIPAA may use third-party tracking tools, such as Google Analytics or Meta Pixel, they can do so only in a very limited way:

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.***¹⁰

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

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.***¹¹

20. Further, Defendant breached its statutory and common law obligations to

¹⁰ *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>, HHS.GOV (last visited May 29, 2023) (noting that “HIPAA Identifiers” include name; address (all geographic subdivisions smaller than state, including street address, city county, and zip code); all elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age); telephone numbers; email address; medical record number; health plan beneficiary number; account number; device identifiers and serial numbers; web URL; internet protocol (IP) address; and any other characteristic that could uniquely identify the individual).

¹¹ *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, available at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>, HHS.GOV (emphasis added) (last visited May 29, 2023).

Plaintiffs and class members by, *inter alia*: (i) failing to adequately review its marketing programs to ensure its Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share Users' Private Information; (iii) failing to obtain the prior written consent of Plaintiffs and class members to disclose their Private Information to Facebook and/or others before doing so; (iv) failing to take steps to block the transmission of Plaintiffs' and class members' Private Information through Meta Pixels; (v) failing to warn Plaintiffs and class members that their Private Information was being shared with third parties without express consent; and (vi) otherwise failing to design and monitor its Web Properties to maintain the security, confidentiality and integrity of patient Private Information.

21. Despite incorporating the Meta Pixel and Conversions API ("CAPI") into its Website and servers, Banner has never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook.¹² Defendant (or any third parties) did not obtain Plaintiffs' and class members' prior consent before sharing their sensitive and confidential communications and Private Information with third parties such as Facebook.

22. As a result of Defendant's conduct, Plaintiffs and class members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Pixel; (iii) emotional distress and heightened concerns related to the release of Private Information to third parties; (iv) loss of the benefit of the bargain; (v) diminution of value of the Private Information; (vi) statutory damages and (vii) continued and ongoing risk to their Private Information. Plaintiffs

¹² In contrast to Defendant, in recent months several medical providers which have installed the Facebook Pixel on their web properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See, e.g., Cerebral, Inc. Notice of HIPAA Privacy Breach*, available at https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited May 29, 2023); *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies* (Oct. 20, 2022), available at <https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3> (last visited May 29, 2023); *Novant Health notifies patients of potential data privacy incident* (Aug. 12, 2022), available at <https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident.aspx> (last visited May 29, 2023).

1 and the members of the Nationwide Class have a substantial risk of future harm, and thus injury
 2 in fact, due to the continued and ongoing risk of misuse of their Private Information that was
 3 shared by Defendant with third parties.

4 23. Plaintiffs seek, on behalf of themselves and a class of similarly situated persons,
 5 to remedy these harms and therefore assert the following statutory and common law claims
 6 against Banner: (i) Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2511(1),
 7 *et seq.*, Unauthorized Interception, Use and Disclosure; (ii) Violation of Electronic
 8 Communications Privacy Act, 18 U.S.C. § 2511(3)(a), *et seq.*, Unauthorized Divulgence by
 9 Electronic Communications Service; (iii) Violation of A.R.S. §44-1521, *et seq.*; (iv) Common
 10 Law Invasion of Privacy – Intrusion Upon Seclusion; (v) Breach of Confidence; (vi) Violation
 11 of the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; (vii) Violation of the
 12 California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56, *et seq.*; (viii)
 13 Violation of The Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* – Unlawful
 14 Business Practices; (ix) Violation of The Unfair Competition Law (“UCL”), Cal. Bus. & Prof.
 15 Code § 17200, *et seq.* – Unfair Prong; (x) Violation of Florida Security of Communications Act
 16 (“FSCA”), Fla. Stat. 934.01, *et seq.*; (xi) Violation of the Colorado Consumer Protection Act,
 17 Colo. Rev. Stat. Section 6-1-101, *et seq.*

18 **THE PARTIES**

19 24. Plaintiff Cheryl McCulley is, and at all relevant times was, an individual residing
 20 in Susanville, Lassen County, in the State of California. Ms. McCulley used the Web Properties
 21 to search for a doctor, review medical conditions, treatments, and test results, and make
 22 appointments to visit healthcare providers.

23 25. Plaintiff Cindy Freriks is, and has been since June 2022, an individual residing in
 24 Lehigh Acres, Lee County, in the State of Florida. Prior to moving to Lehigh Acres in June
 25 2022, Ms. Freriks was a resident of Denver, Colorado. Ms. Freriks used the Web Properties to
 26 search for a doctor, review medical conditions, treatments, and test results, and make
 27 appointments to visit healthcare providers.

28 26. Plaintiff Rebecca Blount is, and at all relevant times was, an individual residing

1 in Casa Grande, Pinal County, in the State of Arizona. Ms. Blount used the Web Properties to
2 search for a doctor, review and research medical conditions, treatments, and test results, and
3 make appointments to visit a healthcare provider.

4 27. Plaintiff Jill Schreidl is, and at all relevant times was, an individual residing in
5 Loveland, Larimer County, in the State of Colorado. Mrs. Schreidl used the Web Properties to
6 search for a doctor, review and research medical conditions, treatments, and test results, and
7 make appointments to visit a healthcare provider.

8 28. Plaintiff John Schreidl is, and at all relevant times was, an individual residing in
9 Loveland, Larimer County, in the State of Colorado. Mr. Schreidl used the Web Properties to
10 search for a doctor, review and research medical conditions, treatments, and test results, and
11 make appointments to visit a healthcare provider.

12 29. Plaintiff Demetria Ann Santiago Laboy (Browning) is, and at all relevant times
13 was, an individual residing in Peoria, Maricopa County, in the State of Arizona. Ms. Laboy
14 (Browning) used the Web Properties to search for a doctor or specialist, review or research
15 medical conditions and treatments, and attempt to make appointments to visit healthcare
16 providers.

17 30. Defendant BANNER HEALTH is incorporated in the State of Arizona, and its
18 principal place of business is located at 2901 N. Central Avenue, Suite 160 in Phoenix, Arizona
19 85012.

20 **JURISDICTION & VENUE**

21 31. This Court has subject matter jurisdiction further to the Class Action Fairness Act
22 of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds \$5 million,
23 exclusive of interest and costs, and minimal diversity exists because at least one class member
24 and Defendant are citizens of different states.

25 32. This Court has federal question jurisdiction further to 29 U.S.C. § 1331 because
26 this complaint alleges violation of federal laws, specifically the Electronic Communications
27 Privacy Act, 18 U.S.C. § 2511(1), *et seq.*

28 33. The Court has personal jurisdiction over Defendant Banner because its principal

place of business and headquarters are located in Phoenix, Arizona, and it regularly engages in extensive business throughout the country and the State of Arizona. Defendant's actions, conduct and omissions emanating in and from its principal offices in Arizona, as described further herein, harmed class members nationwide, including Plaintiffs.

34. Venue is proper in this judicial district pursuant to 18 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in this judicial district and a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this judicial district.

FACTUAL ALLEGATIONS

A. The Use of Tracking Technologies in the Healthcare Industry.

35. Tracking tools¹³ installed on many hospitals', telehealth companies' and other healthcare providers' websites (and other digital properties) are collecting patients' and other visitors' confidential and private health information—including details about their medical conditions, prescriptions and appointments, among *many* other things—and sending that information to third party vendors without prior, informed consent.¹⁴

36. Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to surreptitiously capture and to disclose their Users' personal health information ("PHI").¹⁵

¹³ The Office for Civil Rights at the HHS has defined "tracking technology" as a script or code on a website or mobile app used to gather information about users as they interact with the website or mobile app. After information is collected through tracking technologies from websites or mobile apps, it is then analyzed by owners of the website or mobile app ("website owner" or "mobile app owner"), or third parties, to create insights about users' online activities. *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>, HHS.GOV (last visited May 29, 2023).

¹⁴ *See, e.g.,* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> (last visited May 29, 2023).

¹⁵ *See, e.g.,* Dave Muoio & Annie Burky, *Advocate Aurora, WakeMed get served with class action over Meta's alleged patient data mining*, FIERCE HEALTHCARE (Nov. 4, 2022),

1 37. Specifically, and for example, *The Markup* reported that 33 of the largest 100
 2 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data
 3 whenever a person clicked a button to schedule a doctor’s appointment.¹⁶

4 38. These pixels are snippets of code that track internet users as they navigate through
 5 a website, logging which pages they visit, which buttons they click and certain information they
 6 enter into forms. In exchange for installing the pixels, third party platforms (*e.g.*, Facebook and
 7 Google) provide website owners analytics about the advertisements they have placed as well as
 8 tools to target people who have visited their web properties.

9 39. Of all the information the average internet user shares with the technology
 10 companies, health data is some of the most valuable and controversial. While the information
 11 captured and disclosed without permission may vary depending on the pixel(s) embedded, these
 12 “data packets” can be extensive, sending, for example, not just the name of a physician and field
 13 of medicine, but also the first name, the last name, email address, phone number and zip code
 14 and city of residence entered into the booking form.

15 40. In addition, that data is linked to a specific IP address.¹⁷ The Meta Pixel, for
 16 example, sends information to Facebook via scripts running in a person’s internet browser so
 17 each data packet comes labeled with an IP address that can be used in combination with other
 18
 19
 20

21 [https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-](https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-patient-data-facebook)
 22 [patient-data-facebook](https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-patient-data-facebook) (last visited May 29, 2023).

23 ¹⁶ See note 1.

24 ¹⁷ Even IP addresses—which in theory could be connected to several members of the same
 25 household—are considered PHI *even when the individual does not have an existing relationship*
 26 *with the regulated healthcare entity* since when the medical provider collects this information
 27 through its website or mobile app, it is indicative that the individual has received or will receive
 28 health care services or benefits from the medical provider. See HHS.gov, USE OF ONLINE
 TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES & BUSINESS
 ASSOCIATES, [https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html)
[tracking/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html), HHS.GOV (last visited May 29, 2023).

1 data to identify an individual or household.¹⁸

2 41. Even if Users somehow become aware that a given website is utilizing pixels to
3 collect and to disseminate their data without permission, the third-party platforms have designed
4 (and the site owners have implemented) workarounds that cannot be evaded by savvy users.

5 42. Facebook’s workaround, for example, is called Conversions API. CAPI is an
6 effective workaround because it does not intercept data communicated from the user’s browser;
7 rather, CAPI “is designed to create a direct connection between [Web hosts’] marketing data
8 and [Facebook].” Thus, the (supposedly) private communications between patients and
9 Defendant, which are necessary to use Website, are actually received by Defendant and stored
10 on its server before CAPI collects and sends the Private Information contained in those
11 communications directly from Defendant to Facebook. Client devices do not have access to host
12 servers and thus cannot prevent (or even detect) this transmission.¹⁹

13 43. Thus, without any knowledge, authorization or action by a User, a website owner
14 (like Banner) can use its source code to commandeer a user’s computing device, causing the
15 device to contemporaneously and invisibly re-direct the users’ communications to third parties.

16 44. In this case, Banner employed the Meta Pixel and, upon information and good
17 faith belief, CAPI and/or other similar technologies, to intercept, duplicate and re-direct
18 Plaintiffs’ and Class Members’ Private Information to third parties like Facebook and Google.

19 ***B. Banner Discloses Plaintiffs’ and Class Members’ Private Information to Facebook.***

20
21 ¹⁸ In addition, if the person is (or recently has) logged into Facebook when they visit a
22 particular website, some browsers will attach third-party cookies—another tracking
mechanism—that allow Meta to link pixel data to specific Facebook accounts.

23 ¹⁹ While there is no way to confirm with certainty that a Web host like Defendant has
24 implemented workarounds like CAPI without access to the host server, companies like
25 Facebook instruct the companies it partners with to “[u]se the Conversions API in addition to
26 the [] Pixel, and share the same events using both tools,” because such a “redundant event setup”
allows Defendant “to share website events [with Facebook] that the pixel may lose.” Thus, it is
27 reasonable to infer that Facebook’s customers who implement the Meta Pixel in accordance with
28 Facebook’s documentation will also implement the Conversions API workaround. *See Best
practices for Conversions API*,
<https://www.facebook.com/business/help/308855623839366?id=818859032317965>,
FACEBOOK.COM (last visited May 29, 2023).

1 45. Banner offers an array of services including behavioral and mental health,
2 Alzheimer's, cancer and diabetes care, and other medical treatments and services.²⁰

3 46. Defendant uses the Website to connect Plaintiffs and Class Members to its digital
4 healthcare platforms with the goal of increasing profitability.

5 47. Defendant purposely installed the Pixel and other tracking tools on its Web
6 Properties and programmed the Properties to surreptitiously share its patients' private and
7 protected communications with Facebook, including communications that contain Plaintiffs'
8 and Class Members' Private Information.

9 48. In order to understand Defendant's unlawful data sharing practices, it is important
10 to first understand basic web design and tracking tools.

11 49. Facebook operates the world's largest social media company and generated \$117
12 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.²¹

13 50. In conjunction with its advertising business, Facebook encourages and promotes
14 entities and website owners, such as Defendant, to utilize its "Business Tools" to gather,
15 identify, target, and market products and services to individuals.

16 51. Facebook's Business Tools, including the Pixel, are bits of code that advertisers
17 can integrate into their webpages and servers, thereby enabling the interception and collection
18 of user activity on those platforms.

19 52. The Business Tools are automatically configured to capture "Standard Events"
20 such as when a user visits a particular webpage, that webpage's Universal Resource Locator
21 ("URL") and metadata, button clicks, etc.²²

22 ²⁰ <https://www.bannerhealth.com/services/service-listing> (last visited May 29, 2023).
23

24 ²¹ META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS,
25 <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx>, INVESTOR.FB.COM (last visited May 29, 2023).
26

27 ²² *Specifications for Facebook Pixel Standard Events*,
28 <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>,
FACEBOOK.COM (last visited May 29, 2023); *see*, META PIXEL, GUIDES, ADVANCED,

53. Notably, advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a “custom event.”²³

54. One such Business Tool is the Meta Pixel which “tracks the people and type of actions they take.”²⁴ When a user accesses a webpage with the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook’s servers—traveling from the user’s browser to Facebook’s server.

55. Notably, this transmission only occurs on webpages that contain the Pixel. Thus, Plaintiffs’ and Class Member’s Private Information would not have been disclosed to Facebook but for Defendant’s decision to install the Pixel on its Website.

56. Similarly, Plaintiffs’ and Class Member’s Private Information would not have been disclosed to Facebook via CAPI but for Defendant’s decision to install and implement that tool on its Web Properties.

57. By installing and implementing both tools, Defendant caused Plaintiffs’ and Class Member’s communications to be intercepted and transmitted to Facebook via the Pixel, and it caused a second improper disclosure of that information via CAPI.

58. As explained below, these unlawful transmissions are initiated by Defendant’s source code concurrent with communications made via the Website.

C. Banner’s Method of Transmitting Plaintiffs’ & Class Members’ Private Information via the Meta Pixel and/or CAPI.

<https://developers.facebook.com/docs/facebook-pixel/advanced/>, FACEBOOK.COM (last visited May 29, 2023); *see also* BEST PRACTICES FOR META PIXEL SETUP, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>, FACEBOOK.COM (last visited May 29, 2023); META MARKETING API, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/> FACEBOOK.COM (last visited May 29, 2023).

²³ ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>, FACEBOOK.COM (last visited May 29, 2023); *see also* META MARKETING API, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/>, FACEBOOK.COM (last visited May 29, 2023).

²⁴ RETARGETING, <https://www.facebook.com/business/goals/retargeting>, FACEBOOK.COM (last visited May 29, 2023).

59. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each “client device” (such as computer, tablet, or smart phone) accesses 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).

60. Every website is hosted by a computer “server” that holds the website’s contents and through which the entity in charge of the website exchanges communications with Internet users’ client devices via web browsers.

61. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **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.
- **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 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 when visiting one website to 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.²⁵

62. A patient’s HTTP Request essentially asks the Defendant’s Website to retrieve certain information (such as a physician’s “Book an Appointment” page), and the HTTP Response renders or loads the requested information in the form of “Markup” (the pages, images, words, buttons, and other features that appear on the patient’s screen as they navigate Defendant’s Website).

63. Every website is comprised of Markup and “Source Code.” Source Code is a set

²⁵ One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

1 of instructions that commands the website visitor's browser to take certain actions when the web
2 page first loads or when a specified event triggers the code.

3 64. Source Code may also command a web browser to send data transmissions to third
4 parties in the form of HTTP Requests quietly executed in the background without notifying the
5 web browser's user. The Pixel Defendant uses Source Code that does just that. The Pixel acts
6 much like a traditional wiretap.

7 65. When patients visit Defendant's Web Properties via an HTTP Request to Banner's
8 server, that server sends an HTTP Response including the Markup that displays the Webpage
9 visible to the user and Source Code including Defendant's Pixel.

10 66. Thus, Defendant is, in essence, handing patients a tapped device and once the
11 Webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for
12 private communications on the Webpage to trigger the tap, which intercepts those
13 communications—intended only for Defendant—and transmits those communications to third
14 parties, including Facebook and Google. Such conduct occurs on a continuous, and not
15 sporadic, basis.

16 67. Third parties, like Facebook, place third-party cookies in the web browsers of
17 users logged into their services.

18 68. These cookies uniquely identify the user and are sent with each intercepted
19 communication to ensure the third-party can uniquely identify the patient associated with the
20 Personal Information intercepted.

21 69. With substantial work and technical know-how, internet users can sometimes
22 circumvent this browser-based wiretap technology. This is why third parties bent on gathering
23 Private Information, like Facebook, implement workarounds that cannot be evaded by savvy
24 users.

25 70. Facebook's workaround, for example, is called CAPI, which is an "effective"
26 workaround because it does not intercept data communicated from the user's browser. Instead,
27 CAPI "is designed to create a direct connection between [Web hosts'] marketing data and
28 [Facebook]."

71. Thus, the communications between patients and Defendant, which are necessary to use Defendant's Website, are actually received by Defendant and stored on its server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Facebook.

72. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

73. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like CAPI without access to the host server, companies like Facebook instruct Defendant to "[u]se the CAPI in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."²⁶

74. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner (i.e., to bolster profits).

75. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly redirect the Users' communications to third parties.

76. In this case, Defendant employed the Tracking Pixel and CAPI to intercept, duplicate and re-direct Plaintiffs' and Class Members' Private Information to Facebook.

77. For example, when a patient visits www.bannerhealth.com and enters "HIV & AIDS" into the search bar, the patient's browser automatically sends an HTTP Request to Defendant's web server. The Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage as depicted below.

²⁶ See *Best practices for Conversions API*, <https://www.facebook.com/business/help/308855623839366?id=818859032317965>, FACEBOOK.COM (last visited May 29, 2023).

Figure 1. Image taken from
<https://www.bannerhealth.com/search?query=HIV%20%26%20AIDS>

78. The patient visiting this particular web page only sees the Markup, not the Defendant's Source Code or underlying HTTP Requests and Responses.

79. In reality, Defendant's Source Code and underlying HTTP Requests and Responses share the patient's personal information with Facebook, including the fact that the patient is looking for treatment for HIV and/or AIDS—along with the patient's unique Facebook identifiers.

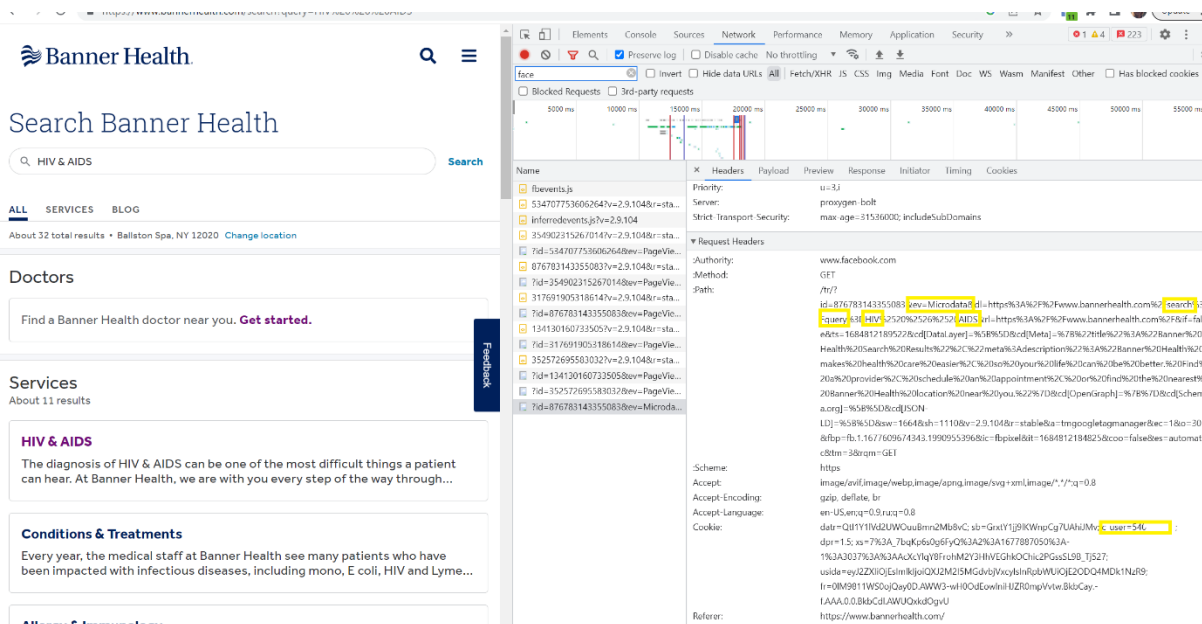


Figure 2. An HTTP single communication session sent from the device to Facebook that reveals the user's search terms along with the user's unique Facebook personal identifier (the `c_user` field).²⁷

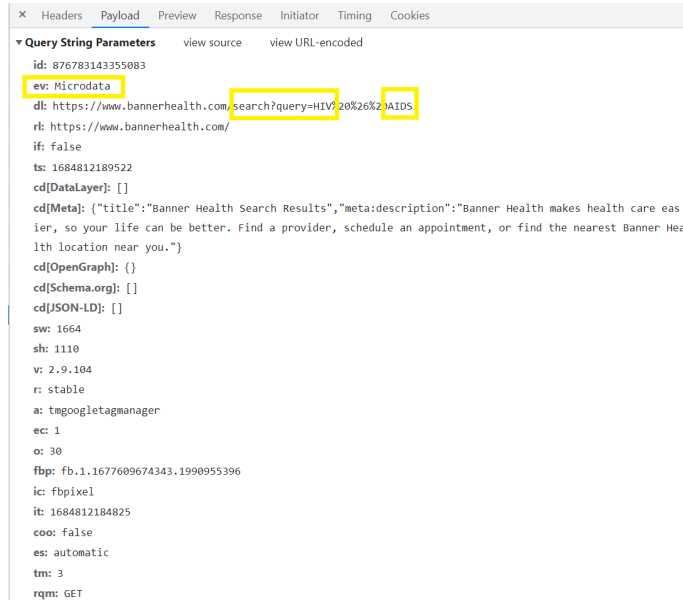


Figure 3. An easier-to-read representation of data sent to Facebook when a user enters search terms into the search bar.

80. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions and can command a website visitor's browser to send data transmissions to third parties via pixels or web bugs,²⁸ effectively open a spying window through which the webpage can funnel the visitor's data, actions, and communications to third parties.

81. Looking to the previous example, Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) and sending those communications to Facebook.

82. This occurs because the Pixel embedded in Defendant's Source Code is programmed to automatically track and transmit a patient's communications, and this occurs

²⁷ One of the user's personal identifiers from Facebook, the FID (represented as the `c_user` cookie highlighted in the image above), has been redacted to preserve the user's anonymity.

²⁸ These pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware of them.

1 contemporaneously, invisibly and without the patient's knowledge.

2 83. Thus, without its patients' consent, Defendant has effectively used its source code
3 to commandeer patients' computing devices thereby re-directing their Private Information to
4 third parties.

5 84. The information that Defendant's Pixel sends to Facebook may include, among
6 other things, patients' PII, PHI and other confidential information.

7 85. Consequently, when Plaintiff and Class Members visit Defendant's website and
8 communicate their Private Information, it is transmitted to Facebook, including, but not limited
9 to, patient status, health conditions experienced and treatments sought, physician selected,
10 specific button/menu selections, and appointment type and date.

11 ***D. Defendant's Pixel and/or CAPI Tracking Practices caused Plaintiffs' & Class***
12 ***Members' PII & PHI to be sent to Facebook.***

13 86. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel
14 and/or CAPI on its Web Properties to secretly track patients by recording their activity and
15 experiences in violation of its common law, contractual, statutory and regulatory duties and
16 obligations.

17 87. Defendant's Web Pages contain a unique identifier which indicates that the Pixel
18 is being used on a particular webpage.²⁹

19 88. The Pixels allow Defendant to optimize the delivery of ads, measure cross-device
20 conversions, create custom audiences and decrease advertising and marketing costs.

21 89. However, Defendant's Web Properties do not rely on the Pixel in order to
22 function.

23 90. While seeking and using Defendant's services as a medical provider, Plaintiffs
24 and Class Members communicated their Private Information to Defendant via its Web
25 Properties.

26
27 ²⁹ Defendant's Website has more than one Meta Pixel installed on various webpages,
28 including those identified as 134130160733505, 317691905318614, 352572695583032,
354902315267014, 534707753606264, and 876783143355083 on www.bannerhealth.com.

1 91. Defendant did not disclose to Plaintiff and Class Members that their Private
2 Information would be shared with Facebook as it was communicated to Defendant. Rather,
3 Defendant represented the opposite. This prevents the provision of any informed consent by
4 Plaintiffs or members of the Class to Defendant for the challenged conduct described herein.

5 92. Plaintiffs and Class Members never consented, agreed, authorized or otherwise
6 permitted Defendant to disclose their Private Information to Facebook (or any other third-party),
7 nor did they intend for Facebook to be a party to their communications with Defendant.
8 Defendant does not employ any form or click system whereby Plaintiffs and Class Members
9 provide their affirmative consent to Defendant agreeing, authorizing or otherwise permitting
10 Defendant to disclose their Private Information to Facebook (or any other third-party).

11 93. Defendant's Pixels and CAPI sent non-public Private Information to Facebook,
12 including but not limited to Plaintiffs' and Class Members': (i) status as medical patients; (ii)
13 health conditions; (iii) sought treatment or therapies; (iv) terms and phrases entered into
14 Defendant's search bar; (v) medical classes requests and medical classes booking information;
15 (vi) locations or facilities where treatment is sought; and (vii) which web pages were viewed.

16 94. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent
17 alongside Plaintiffs' and Class Members' personal identifiers, including patients' IP address and
18 cookie values thereby allowing individual patients' communications with Defendant, and the
19 Private Information contained in those communications, to be linked to their unique Facebook
20 accounts.

21 95. Through the source code deployed by Defendant, the cookies that it uses to help
22 Facebook identify patients include but are not necessarily limited to cookies named: c_user,
23 datr, fr, and fbp.³⁰

24 _____
25 ³⁰ Defendant's Website tracks and transmits data via first-party and third-party cookies.
26 C_user, datr, and fr cookies are third-party cookies. The fbp cookie is a Facebook identifier that
27 is set by Facebook source code and associated with Defendant's use of the Facebook Pixel. The
28 fbp cookie emanates from Defendant's Website as a putative first-party cookie, but is
transmitted to Facebook through cookie syncing technology that hacks around the same-origin
policy.

1 96. The c_user cookie or FID is a type of third-party cookie assigned to each person
2 who has a Facebook account and it is composed of a unique and persistent set of numbers.

3 97. A user's FID is linked to their Facebook profile, which generally contains a wide
4 range of demographic and other information about the user, including pictures, personal
5 interests, work history, relationship status, and other details. Because the user's Facebook
6 Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary
7 person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view
8 the user's corresponding Facebook profile.

9 98. The datr cookie identifies the patient's specific web browser from which the
10 patient is sending the communication. It is an identifier that is unique to the patient's specific
11 web browser and is therefore a means of identification for Facebook users. Facebook keeps a
12 record of every datr cookie identifier associated with each of its users, and a Facebook user can
13 obtain a redacted list of all datr cookies associated with his or her Facebook account from
14 Facebook.

15 99. The fr cookie is a Facebook identifier that is an encrypted combination of the
16 c_user and datr cookies.³¹

17 100. Defendant deprived Plaintiff and Class Members of their privacy rights when it:
18 (i) implemented technology (i.e., the Meta Pixel) that surreptitiously tracked, recorded and
19 disclosed Plaintiffs' and other online patients' confidential communications and Private
20 Information; (ii) disclosed patients' protected information to Facebook—an unauthorized third-
21 party and (iii) undertook this pattern of conduct without notifying Plaintiffs or Class Members
22 and without obtaining their express written consent.

23 ***E. Defendant's Pixel Disseminates Patient Information Via www.Bannerhealth.com***

24 101. If a patient uses www.bannerhealth.com to look for medical treatments, they may
25 select "Cancer" under the "Services" tab, which takes them to the list of services offered by

26 ³¹ See Gunes Acar, Brendan Van Alsenoy, Frank Piessens, Claudia Diaz, and Bart Preneel,
27 Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy
28 Commission (March 27, 2015) (available at https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf) (last visited May 29, 2023).

1 Defendant to cancer patients. On this page the patient can further narrow their search results by
2 cancer programs offered by Banner, clinical trials and research, cancer type, and Banner
3 locations offering cancer treatments, including telehealth options.

4 102. The patient's selections and filters are transmitted to Facebook via the Meta
5 Pixels, even if they contain the patient's treatment, procedures, medical conditions, or related
6 queries.

7 103. This information is automatically sent from the patient's device to Facebook, and
8 it reveals the patient's personal identifiers, including but not limited to, their IP address, FID,
9 datr and fr cookies, along with the search filters the patient selected.

10 104. Defendant's Pixels send each and every communication the user made to the
11 Defendant via the Webpage to Facebook, without alerting the user, and the images below
12 confirm that the communications Defendant sends to Facebook contain the user's Private
13 Information.

14 105. For example, a breast cancer patient can search for breast cancer programs, breast
15 reconstruction surgery, or relevant clinical trials.

16 106. Their selections or search parameters are automatically transmitted by the Pixel to
17 Facebook along with the user's unique personal identifiers, as evidenced by the images below.

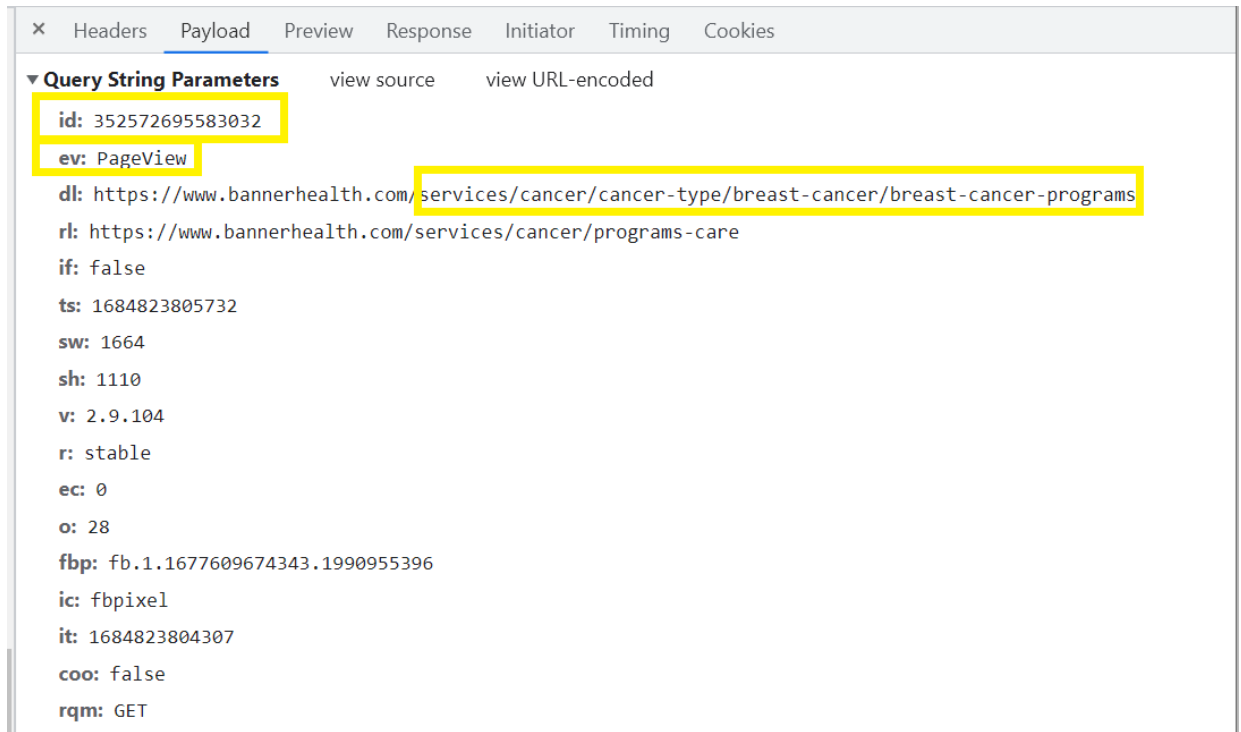


Figure 5. Defendant's transmission to Facebook of patient's search parameters showing condition search terms.

107. The first line of highlighted text, "id: 352572695583032," refers to the Defendant's Pixel ID for this particular Webpage and confirms that the Defendant has downloaded the Pixel into its Source Code on this particular Webpage.

108. The second line of text, "ev: PageView," identifies and categorizes which actions the user took on the Webpage ("ev:" is an abbreviation for event, and "PageView" is the type of event). Here, this event identifies the user as having viewed the particular Webpage.

109. The remaining lines of text identify: (i) the user as a patient seeking medical care from Defendant via www.Bannerhealth.com; (ii) who has breast cancer and (iii) who is searching for breast cancer programs.

110. Finally, the last line of highlighted text ("GET"), demonstrates that Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the user's personal identifiers including Facebook cookies. This is further evidenced by the image below, which was collected during the same browsing session as the previous image.

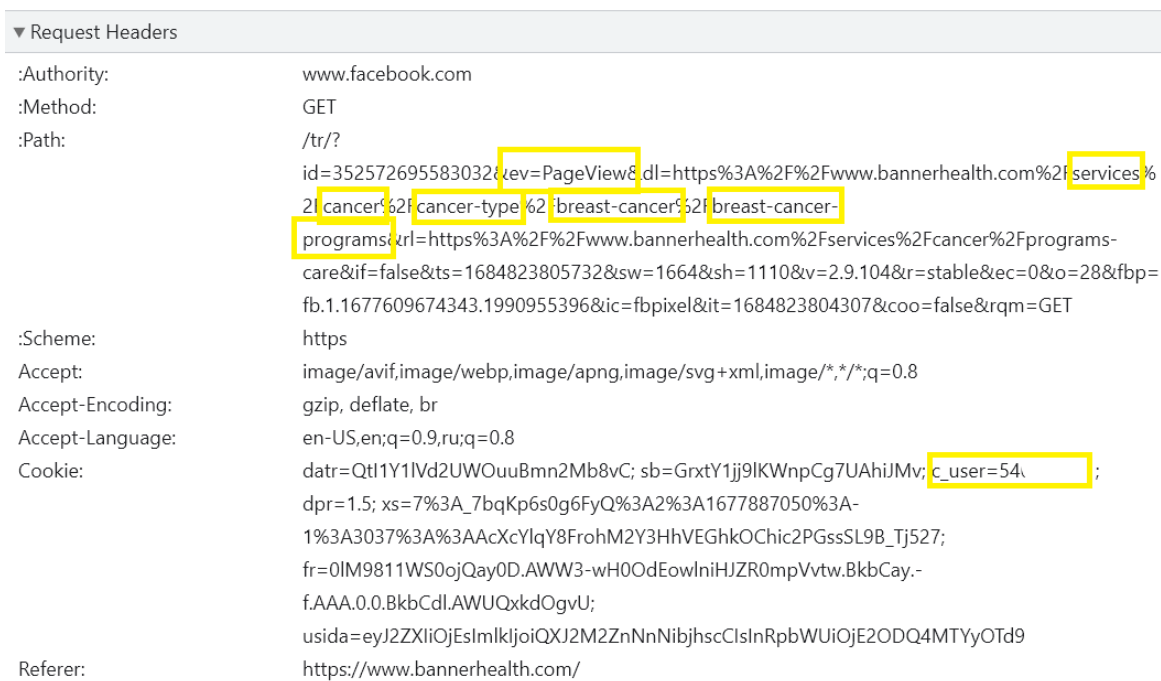


Figure 6. Defendant's transmission to Facebook of patient's search parameters showing search terms and the patient's personal Facebook identifiers including the c_user field.

111. As mentioned above, if the patient selects other cancer services, such as breast reconstruction surgery or clinical trials, those search parameters are also automatically transmitted to Facebook by Defendant's Pixel, along with the patient's personal identifiers.

Figures 7 & 8. HTTP communication sessions sent from the user's device to Facebook revealing the user's search parameters and their personal identifiers.

25

is information is shared with Facebook as shown in the images below:

▼ Query String Parameters view source view URL-encoded

```

id: 876783143355083
ev: SubscribedButtonClick
dl: https://www.bannerhealth.com/services/cancer
rl: https://www.bannerhealth.com/services
if: false
ts: 1684855948523
cd[buttonFeatures]: {"classList": "text-card-link", "destination": "https://www.bannerhealth.com/services/cancer/cancer-type/lung-cancer", "id": "", "imageUrl": "", "innerText": "Lung Cancer\n\nHelping everyone breathe easier.", "numChildButtons": 0, "tag": "a", "type": null, "name": ""}
cd[buttonText]: Lung Cancer

Helping everyone breathe easier.
cd[formFeatures]: []
cd[pageFeatures]: {"title": "Cancer Care & Treatment Options | Banner MD Anderson"}
sw: 1664
sh: 1110
v: 2.9.104
r: stable
a: tmgoogletagmanager
ec: 2
o: 30
fbp: fb.1.1677609674343.1990955396
cs_est: true
ic: fbpixel
it: 1684824958747
coo: false
es: automatic
tm: 3
rqm: GET

```

▼ Request Headers

```

:Authority: www.facebook.com
:Method: GET
:Path: /tr/?
id=876783143355083&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.bannerhealth.com%2Fservices%2Fcancer&rl=https%3A%2F%2Fwww.bannerhealth.com%2Fservices&if=false&ts=1684855948523&cd[buttonFeatures]=%7B%22classList%22%3A%22text-card-link%22%2C%22destination%22%3A%22https%3A%2F%2Fwww.bannerhealth.com%2Fservices%2Fcancer%2Fcancer-type%2Flung-cancer%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Lung%20Cancer%5Cn%5CnHelping%20everyone%20breathe%20easier.%22%2C%22numChildButtons%22%3A%220%22%2C%22tag%22%3A%22a%22%2C%22type%22%3A%22null%22%2C%22name%22%3A%22%22%2C%22cd[buttonText]=Lung%20Cancer%0A%0AHelping%20everyone%20breathe%20easier.&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22Cancer%20Care%20%26%20Treatment%20Options%20%2C%20Banner%20MD%20Anderson%22%2C%22sw=1664&sh=1110&v=2.9.104&r=stable&a=tmgoogletagmanager&ec=2&o=30&fbp=fb.1.1677609674343.1990955396&cs_est=true&ic=fbpixel&it=1684824958747&coo=false&es=automatic&tm=3&rqm=GET
:Scheme: https
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*;*/q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,ru;q=0.8
Cookie: datr=Qt1Y1Ivd2UW0uuBmn2Mb8vC; sb=GrxtY1jj9IKWnpCg7UAhiJMv; c_user=54C; dpr=1.5; xs=7%3A_7bqKp6s0g6fyQ%3A2%3A1677887050%3A-1%3A3037%3A3AAcXcYlqY8FrohM2Y3HhVEGhkoChic2PGssSL9B_Tj527; fr=0lM9811WS0jQay0D.AWW3-wH0OdEowlniHJR0mpVvtw.BkbCay.-f.AAA.0.0.BkbCdl.AWUQxkdOgvU; usida=eyJ2ZXliOjE5mlkljoiQXJ2M2ZnNnNibjhscCIsInRpbWUiOjE2ODQ4MTYyOTd9
Referer: https://www.bannerhealth.com/

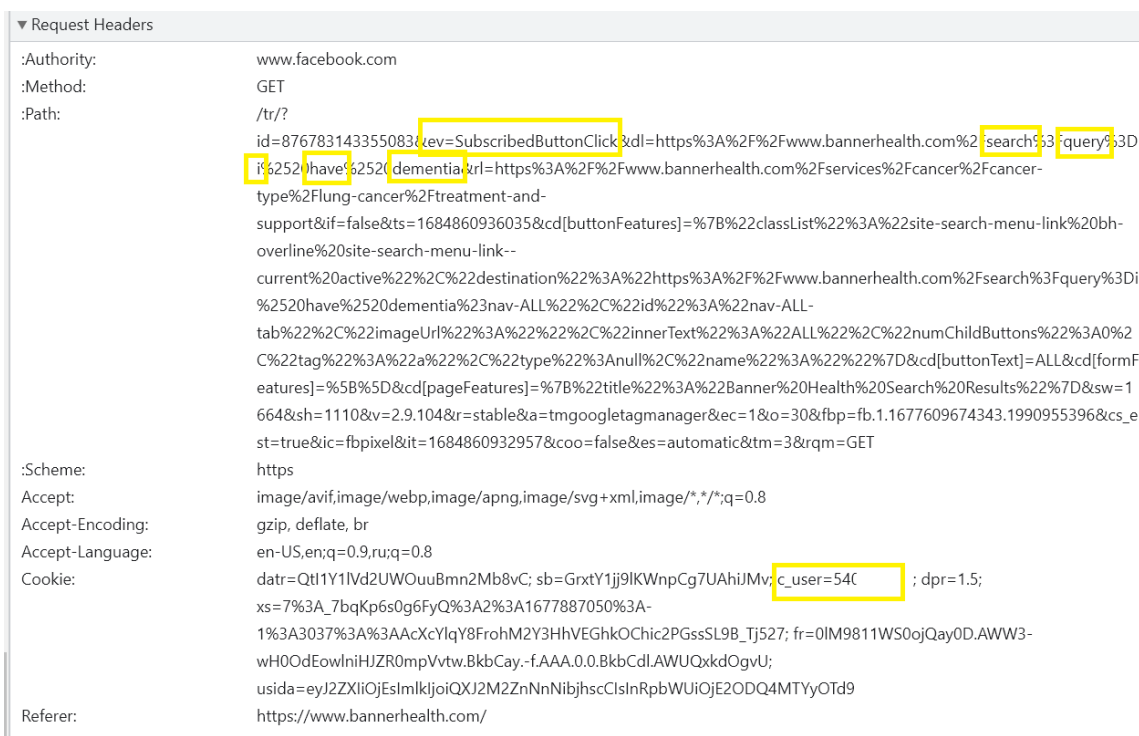
```

Figures 9 & 10. HTTP communication sessions sent from the user's device to Facebook revealing the inner text of button clicked by the user, along with their personal identifiers.

113. To make matters worse, the text and phrases that users type into the search bar are

[illegible]

27



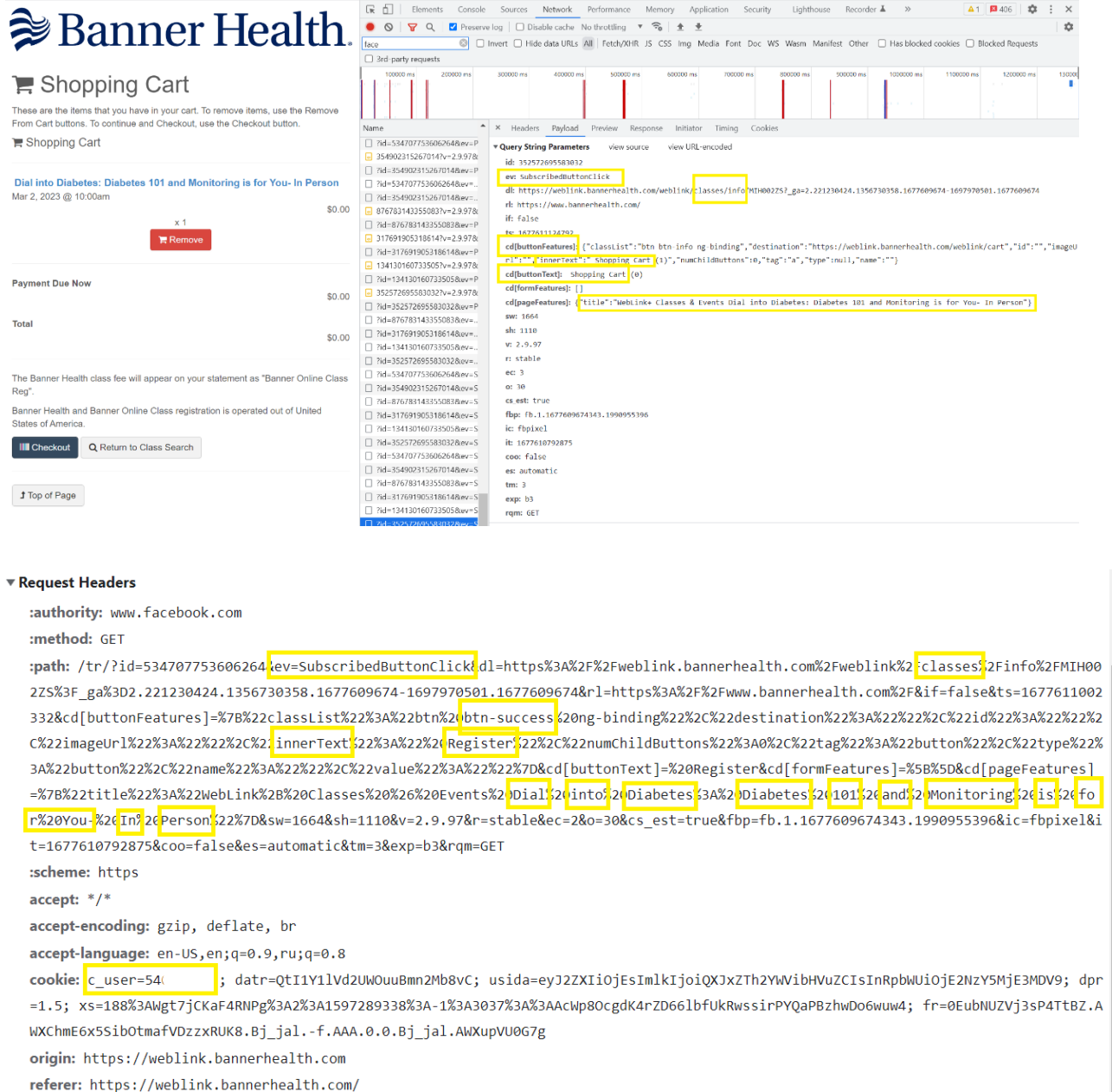
Figures 11 & 12. Example of exact text and phrases being shared with Facebook.

115. Each time Defendant sends this activity data, it also discloses a patient's PII alongside the contents of their communications.

116. Defendant also offers medical classes for patients with specific medical conditions - and shares personal medical information of those users who sign up for the classes.

117. For example, if a patient with diabetes decides to register for Defendant's "Dial Into Diabetes: Diabetes 101 and Monitoring is for You- In Person" class, Defendant shares with Facebook every step of the process, starting with the patient clicking a button to add the class to their "shopping cart" and ending with the confirmation of their registration, which includes the patient's hashed first and last name, phone number, and email.³³

³³ In some instances forms located on webpages with embedded Pixels will send users' personal information like name, phone and email, to Facebook in a "hashed" form (essentially a long string of numbers and letters) which is supposed to be like a more secure pseudonym for the personal information submitted by a user. However, not only does hashing fail to truly protect people's personal information, but Facebook explicitly says that after getting this hashed information, it uses its "advanced matching feature" to link the information with a specific



Figures 13 & 14. Examples of Defendant sharing that a user added a specific Diabetes class to their “Shopping Cart” and then successfully registered for it.

person. See <https://themarkup.org/levelup/2023/01/31/in-2023-resolve-to-fix-your-organizations-meta-pixel-problem> (last visited May 23, 2023).

118. A user who accesses Defendant's website while logged into Facebook will transmit the c_user cookie to Facebook, which contains that user's unencrypted Facebook ID, and other personal cookie values including the datr and fr cookies.

119. When accessing www.Bannerhealth.com, for example, Facebook receives as many as seven cookies:

Request Cookies ☐ show filtered out request cookies

Name	Value	Domain	Path	Expires / Ma...
datr	Qtl...	.facebook.com	/	2024-04-05T...
sb	Grxt...	.facebook.com	/	2024-04-06T...
c_user	540...	.facebook.com	/	2024-05-22T...
dpr	1.5	.facebook.com	/	2023-05-26T...
xs	7%...	.facebook.com	/	2024-05-22T...
fr	0IM...	.facebook.com	/	2023-08-21T...
usida	eyJ...	.facebook.com	/	Session

Figure 15.

120. When a visitor's browser has recently logged out of their Facebook account, Facebook compels the visitor's browser to send a smaller set of cookies³⁴:

fr	00Zp...	.facebook.com
wd	1156...	.facebook.com
sb	qqAz...	.facebook.com
datr	Malz...	.facebook.com

Figure 16.

121. The fr cookie contains, at least, an encrypted Facebook ID and browser identifier.³⁵ Facebook, at a minimum, uses the fr cookie to identify users.³⁶

³⁴ The screenshot below serves as an example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here and in the preceding image is the _fbp cookie, which is transmitted as a first-party cookie.

³⁵ Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit* (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited May 29, 2023).

³⁶ *Cookies & other storage technologies*, FACEBOOK.COM, <https://www.facebook.com/policy/cookies/> (last visited May 29, 2023).

122. At each stage, Defendant also utilized the `_fbp` cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user:³⁷

Name	Value	Domain	P..	Expires / M...
<code>_fbp</code>	fb.1.1677609674343.1990955396	.bannerhealth.com	/	2023-05-2...

Figure 17.

123. The `fr` cookie expires after 90 days unless the visitor's browser logs back into Facebook.³⁸ If that happens, the time resets, and another 90 days begins to accrue.

124. The `_fbp` cookie expires after 90 days unless the visitor's browser accesses the same website.³⁹ If that happens, the time resets, and another 90 days begins to accrue.

125. The Facebook Tracking Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—i.e., Defendant.⁴⁰

126. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook.⁴¹

127. The `_fbp` cookie is always transmitted as a first-party cookie. A duplicate `_fbp` cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

128. Facebook, at a minimum, uses the `fr`, `_fbp`, and `c_user` cookies to link to FIDs and corresponding Facebook profiles.

129. As shown in the figures above, Defendant sent these identifiers with the event

³⁷ *Id.*

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *First-Party Cookie*, PCMAG.COM, <https://www.pcmag.com/encyclopedia/term/first-party-cookie> (last visited May 29, 2023). This is confirmable by using developer tools to inspect a website's cookies and track network activity.

⁴¹ *Third-Party Cookie*, PCMAG.COM, <https://www.pcmag.com/encyclopedia/term/third-party-cookie> (last visited May 29, 2023). This is also confirmable by tracking network activity.

1 data.

2 130. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendant
3 to disclose their PII and PHI nor did they authorize any assistance with intercepting their
4 communications.

5 131. Plaintiffs were never provided with any written notice that Defendant disclosed
6 its Website users' PHI nor were they provided any means of opting out of such disclosures.

7 132. Despite this, Defendant knowingly and intentionally disclosed Plaintiffs' PHI to
8 Facebook.

9 ***F. Banner Does Not Disclose That It Sends Private Information to Third Parties for***
10 ***Marketing Purposes.***

11 133. Banner represents to patients and visitors to its Website that it will only disclose
12 PHI provided to it under certain circumstances, ***none of which apply here.***⁴²

13 133. Defendant's privacy policies do ***not*** permit Defendant to use and disclose
14 Plaintiffs' and Class Members' Private Information for marketing purposes. In fact, Banner
15 acknowledges in its "Notice of Privacy Practices" that it must obtain Users' "written
16 authorization" to use or to disclose PHI; moreover, specific examples of uses or disclosures that
17 require written authorization emphasize "sale of medical information."⁴³ Further, in its Health
18 Privacy Statement Defendant states: "We do not sell User Information to third parties."⁴⁴ Any
19 "limited circumstances" listed as exceptions do not apply to the challenged practices described
20 herein.

21 134. Not only does Banner state that it will not disclose its Users' protected medical
22 information, it also ***falsely represents that it does not utilize Pixels on its Website*** – whereas
23 Defendant's Webpages, including the one with this false representation, have as many as six
24 embedded Pixels collecting and sharing various types of Users' PI:

25 ⁴² <https://www.bannerhealth.com/about/legal-notices/privacy> (last visited May 29, 2023).

26 ⁴³ <https://www.bannerhealth.com/-/media/files/project/bh/patients-visitors/privacy-practices/hipaa-eng-fs-03-28-19.ashx> (last visited May 29, 2023).

27 ⁴⁴ <https://www.bannerhealth.com/about/legal-notices/privacy>.

Pixel Tags or Clear GIFs, also known as Web Beacons or Web Bugs, are transparent graphical images placed on a website. Currently, Banner Health does not use them on its site.



135. Defendant violated its own privacy policy by unlawfully intercepting and disclosing Plaintiffs' and Class Members' Private Information to Facebook and third parties without adequately disclosing that it shared Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

136. The Pixel, which is embedded in and throughout the Website, collects search queries regarding users' personal information including their name and email, their medical conditions, treatment and/or specific providers. Even non-Facebook users can be individually identified via the information gathered on the Web Properties, like an IP address or personal device identifying information.⁴⁵

137. In fact, in an action currently pending against Facebook related to use of their Pixel on healthcare provider web properties, Facebook explicitly stated it requires Pixel users to "post a prominent notice on every page where the pixel is embedded and to link from that notice to information about exactly how the pixel works and what is being collected through it, so it is not invisible."⁴⁶ Defendant not only did not post such a notice but, as demonstrated herein, falsely represented it does not use Pixels on its Website.

138. Facebook further stated that "most providers [...] will not be sending [patient information] to Meta because it violates Meta's contracts for them to be doing that."⁴⁷

139. Facebook also admitted that if patients want to prevent Facebook from tracking them on healthcare provider web properties, to do so, "they can pick up the telephone," i.e., call to make their appointments etc. instead of using the services of the web properties.⁴⁸

⁴⁵ This is precisely the type of information for which HIPAA requires the use of de-identification techniques to protect patient privacy. See <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>, HHS.GOV (last visited May 29, 2023).

⁴⁶ See Transcript of the argument on Plaintiff's Motion for Preliminary Injunction in *In re Meta Pixel Healthcare Litigation*, Case No. CV-22-03580-WHO (N.D. Cal. Nov. 9, 2022) (Hon. J. Orrick), attached hereto as Exhibit A, at 19:12-18. See also *In re Meta Pixel Healthcare Litig.*, - F.Supp.3d -, 2022 WL 17869218 (N.D. Cal. Dec 22, 2022).

⁴⁷ *Id.*, 7:20- 8:11.

⁴⁸ *Id.*, 8:22-23:3.

G. Banner's Disclosure of PHI Without Informed Consent Violates HIPAA's Privacy Rule & OCR Guidance.

140. Beyond Defendant's own policies, and those of Meta, the government has issued guidance warning that tracking code like Meta Pixel may come up against federal privacy law when installed on healthcare websites. The statement, titled *Use of Online Tracking Technologies By HIPAA Covered Entities And Business Associates* (the "Bulletin"), was recently issued by the HHS' Office for Civil Rights ("OCR").⁴⁹

141. Healthcare organizations regulated under the HIPAA may use third party tracking tools, such as Google Analytics or Meta Pixel, in a limited way, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors. The Bulletin explains:

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.***⁵⁰

142. The bulletin 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 others. 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 others 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***

⁴⁹ *Use Of Online Tracking Technologies By HIPAA Covered Entities And Business Associates*, HHS.GOV, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited May 29, 2023).

⁵⁰ *Id.* (emphasis added).

*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.*⁵¹

143. Plaintiffs and Class Members face the precise risks the government is warning about as Banner has shared Plaintiffs' 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 healthcare for certain conditions; and where they seek medical treatment.

144. 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:

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.*⁵²

*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.]*⁵³

145. Banner's disclosure of Plaintiffs' and Class Members' Private Information to entities like Facebook violated HIPAA's Privacy Rule, which defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (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

⁵¹ *Id.* (emphasis added).

⁵² *Id.* (emphasis added).

⁵³ *Id.* (emphasis added).

1 provision of health care to an individual;” and either (i) “identifies the individual;” or (ii) “[w]ith
 2 respect to which there is a reasonable basis to believe the information can be used to identify
 3 the individual.” 45 C.F.R. § 160.103.

4 146. HIPAA prohibits health care providers from “us[ing] or disclos[ing] ‘protected
 5 health information “except as permitted or required by” the HIPAA Privacy Rule. *See* 45 C.F.R.
 6 § 164.502.⁵⁴

7 147. Consistent with this restriction, HHS has issued marketing guidance that provides,
 8 “[w]ith limited exceptions, the [Privacy] Rule requires an individual’s written authorization
 9 before a use or disclosure of her or her [PHI] can be made for marketing . . . Simply put, a
 10 covered entity may not sell [PHI] to a business associate or any other third party for that party’s
 11 own purposes. Moreover, covered entities may not sell lists of patients to third parties without
 12 obtaining authorization from each person on the list.”⁵⁵

13 148. Commenting on a June 2022 report discussing the use of the Meta Pixel by
 14 hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior
 15 privacy adviser in HHS OCR, which enforces HIPAA, stated, “I am deeply troubled by what
 16 [the hospitals] are doing with the capture of their data and the sharing of it ... It is quite likely a
 17 HIPAA violation.”⁵⁶

18 149. Defendant’s placing a third-party tracking code on its Web Properties is a
 19 violation of Plaintiffs’ and Class Members’ privacy rights under HIPAA’s Privacy Rule. While
 20 Plaintiffs do not bring a claim under HIPAA itself, this violation demonstrates Banner’s

21 ⁵⁴ Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a
 22 particular entity, can be PHI. The Department of Health and Human Services has instructed
 23 health care providers that, while identifying information alone is not necessarily PHI if it were
 24 part of a public source such as a phonebook because it is not related to health data, “[i]f 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 ⁵⁵ *Marketing*, [https://www.hhs.gov/hipaa/for-](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html)
 26 [professionals/privacy/guidance/marketing/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html), HHS.GOV (last visited May 29, 2023).

27 ⁵⁶ ‘Deeply Troubled’: Security experts worry about Facebook trackers on hospital sites,
 28 ADVISORY BOARD, <https://www.advisory.com/daily-briefing/2022/06/17/data-trackers> (last
 visited May 29, 2023).

wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

150. Tech companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes. For instance, the health data Google collects could eventually help it to micro-target advertisements to people with certain health conditions.

151. Policymakers are proactively calling for a revision and potential upgrade of the HIPAA privacy rules out of concern for what might happen as tech companies continue to march into the medical sector.⁵⁷

152. Similarly, a Time Magazine article titled, *How your Medical Data Fuels A Hidden Multi-Billion Dollar Industry*, referenced the “growth of the big health data bazaar,” in which patients’ health information is sold:

[T]he secondary market in information unrelated to a patient’s direct treatment poses growing risks, privacy experts say. That’s because clues in anonymized patient dossiers make it possible for outsiders to determine your identity, especially as computing power advances in the future.⁵⁸

153. Banner gave away Plaintiffs’ and Class Members’ private communications and transactions on its Web Properties without permission. The unauthorized access to Plaintiffs’ and Class Members’ Private Information has diminished the value of that information, resulting in harm to Users, including Plaintiffs and Class Members.

H. Plaintiffs’ & Class Members’ Expectation of Privacy

151. Plaintiffs and Class Members were aware of Defendant’s duty of confidentiality when they sought medical services from Defendant.

152. Indeed, at all times when Plaintiffs and Class Members provided their PII and PHI to Defendant, they each had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial

⁵⁷ *Id.*

⁵⁸ Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry* (Jan. 9, 2017), TIME, <https://time.com/4588104/medical-data-industry/> (last visited May 29, 2023).

purpose, unrelated to patient care.

I. The Information Banner Discloses to Third Parties Is PHI.

1. IP Addresses are Personally Identifiable Information

153. In addition to patient status, medical conditions, treatment, specific providers, appointment information and patient's unique and persistent Facebook ID, Defendant improperly disclosed patients' computer IP addresses to Facebook through the use of the Pixel.

154. An IP address is a number that identifies the address of a device connected to the Internet.

155. IP addresses are used to identify and route communications on the Internet.

156. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

157. Facebook tracks every IP address ever associated with a Facebook user.

158. Facebook, Google and other third-party marketing companies track IP addresses for use in tracking and targeting individual homes and their occupants with advertising by using IP addresses.

159. Under HIPAA, an IP address is considered personally identifiable information.

160. HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. See 45 C.F.R. § 164.514 (2).

161. HIPAA further declares information as personally identifiable where the covered entity has "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. § 164.514(2)(ii); See also, 45 C.F.R. § 164.514(b)(2)(i)(O).

162. Consequently, Defendant's disclosure of patients' IP addresses violated HIPAA and industry privacy standards.

2. Internet Cookies are Personally Identifiable Information

163. In the early years of the Internet, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports

1 section of a traditional newspaper, advertisers on the early Internet paid for ads to be placed on
2 specific web pages based on the type of content displayed on the web page.

3 164. Computer programmers eventually developed “cookies”—small text files that
4 web servers can place on a person’s web browser and computing device when that person’s web
5 browser interacts with the website server. Cookies can perform different functions, like saving
6 a user’s login or other site settings. Eventually, some cookies were designed to acquire and
7 record an individual Internet user’s communications and activities on websites across the
8 Internet.

9 165. Cookies are designed to and, in fact, most often do operate as a means of
10 identification for Internet users.

11 166. Cookies are protected personal identifiers under HIPAA. *See* 45 C.F.R. §
12 164.514(b)(2)(i)(H), (J), (M), (N), and (R).

13 167. In general, cookies are categorized by (1) duration and (2) party.

14 168. There are two types of cookies classified by duration:

- 15 a. “Session cookies” are placed on a user’s computing device only while the user is
16 navigating the website that placed and accesses the cookie. The user’s web
17 browser typically deletes session cookies when the user closes the browser.
- 18 b. “Persistent cookies” are designed to survive beyond a single Internet browsing
19 session. The party creating the persistent cookie determines its lifespan. As a
20 result, a persistent cookie can acquire and record a user’s Internet
21 communications for years and over dozens or hundreds of websites. Persistent
22 cookies are sometimes called “tracking cookies.”

23 169. Cookies are also classified by the party that uses the collected data.

- 24 a. “First-party cookies” are set on a user’s device by the website with which the
25 user is exchanging communications. For example, Banner sets a collection of its
26 own cookies on patients’ browsers when they visit any webpage on Banner’s web
27 properties. First-party cookies can be helpful to the user, server, and/or website
28 to assist with security, log in, and functionality.

1 b. “Third-party cookies” are set on a user’s device by website servers other than the
2 website or server with which the user is exchanging communications. For
3 example, the same patient who visits www.bannerhealth.com will also have
4 cookies on their device from third parties, such as Facebook. Unlike first-party
5 cookies, third-party cookies are not typically helpful to the user. Instead, third-
6 party cookies are typically used for data collection, behavioral profiling, and
7 targeted advertising.

8 170. Data companies, like Facebook, have developed methods for monetizing and
9 profiting from cookies. These companies use third-party tracking cookies to help them acquire
10 and record user data and communications in order to sell individually customized advertising.
11 Assigning one, or a set, of unique identifiers to each Internet user aids these data companies in
12 constructing such individual profiles.

13 171. Traditionally, first- and third-party cookies were kept separate. An Internet
14 security policy known as the same-origin policy required web browsers to prevent one web
15 server from accessing the cookies of a separate web server. For example, although Banner could
16 deploy source code that uses Facebook third-party cookies to help Facebook acquire and record
17 the patient’s communications, Banner was not permitted direct access to Facebook third-party
18 cookie values. The reverse was also true: Facebook was not provided direct access to the values
19 associated with first party cookies set by Banner.

20 172. Data companies have designed a way to hack around the same-origin policy so
21 that third-party data companies can now gain access to first-party cookies.

22 173. Javascript source code developed by third-party data companies and placed on a
23 webpage by a developer such as Banner can bypass the same-origin policy to send a first-party
24 cookie value in a tracking pixel to the third-party data company. This technique is known as
25 “cookie syncing,” and it allows two cooperating websites to learn each other’s cookie
26 identification numbers for the same user. Once the cookie syncing operation is completed, the
27 two websites can exchange any information they have collected and recorded about the same
28 user that is associated with a cookie identification number. Cookie syncing can also be used to

1 track an individual who has chosen to deploy third-party cookie blockers.

2 174. Whenever a Banner patient uses Defendant's Web Properties, Banner uses and
3 causes the disclosure of patient cookie identifiers with each re-directed communication
4 described herein, including patient status, conditions, treatments sought, location, and
5 appointment details.

6 175. Defendant's cookie disclosures include the deployment of cookie syncing
7 techniques that cause the disclosure of the first-party cookie values that Banner assigns to
8 patients to be made to third parties.

9 **REPRESENTATIVE PLAINTIFFS' EXPERIENCES**

10 ***Plaintiff McCulley's Experience with Banner***

11 176. As a condition of receiving Defendant's services, Plaintiff McCulley disclosed her
12 Private Information to Defendant on numerous occasions, and most recently in March 2023.

13 177. Plaintiff McCulley accessed Defendant's Website and Patient Account on her
14 phone and computer to receive healthcare services from Defendant and at Defendant's direction.

15 178. Plaintiff McCulley researched providers, specific health conditions and
16 treatments, looked for Defendant's locations close to her address, and scheduled doctor's
17 appointments for herself via the Defendant's Website and Account.

18 179. Plaintiff McCulley also utilized Defendant's Account to refill prescriptions, look
19 at her bills and payments and to see her test results.

20 180. Plaintiff McCulley has used and continues to use the same devices to maintain and
21 access an active Facebook account throughout the relevant period in this case.

22 181. Plaintiff McCulley reasonably expected that her communications with Defendant
23 via the Web Properties were confidential, solely between herself and Defendant, and that such
24 communications would not be transmitted to or intercepted by a third party.

25 182. However, and as a result of the Meta Pixel Defendant chose to install on its
26 Website, Plaintiff McCulley's Private Information was intercepted, viewed, analyzed and used
27 by unauthorized third parties.

28 183. Defendant transmitted Plaintiff McCulley's Facebook ID, computer IP address

1 and other device and unique online identifiers to Facebook. Defendant also transmitted
2 information such as health and medical information including Plaintiff's particular health
3 condition, the type of medical treatment sought, patient status and the fact that Plaintiff
4 attempted to or did book a medical appointment.

5 184. Plaintiff McCulley never consented to the disclosure of or use of her Private
6 Information by third parties or to Defendant enabling third parties, including Facebook, to access
7 or interpret such information. Plaintiff McCulley never consented to any third parties' receipt
8 or use of her Private Information.

9 185. Notwithstanding, through the Meta Pixel and similar technologies embedded on
10 Defendant's Website, Defendant transmitted Plaintiff McCulley's Private Information to, at a
11 minimum, Facebook and likely many other third parties like Google, Bing and others.

12 186. By making these disclosures without her consent, Defendant breached Plaintiff
13 McCulley's privacy and unlawfully disclosed her Private Information.

14 187. Defendant did not inform Plaintiff McCulley that it had shared her Private
15 Information with Facebook.

16 188. Plaintiff McCulley used and continues to use the same devices to maintain and to
17 access an active Facebook account throughout the relevant period for this case.

18 189. Plaintiff McCulley has a continuing interest in ensuring that her Private
19 Information, which, upon information and belief, remains backed up in Defendant's possession,
20 is protected and safeguarded from future unauthorized disclosure(s).

21 190. Plaintiff McCulley would consider using Defendant's services again and/or in
22 greater frequency if she could be assured by Defendant that the violations set forth herein were
23 no longer occurring.

24 ***Plaintiff Blount's Experience with Banner***

25 191. As a condition of receiving Defendant's services, Plaintiff Blount disclosed her
26 Private Information to Defendant on numerous occasions, and most recently in April 2023.

27 192. Plaintiff Blount accessed Defendant's Website and Patient Account on her phone
28 and computer to receive healthcare services from Defendant and at Defendant's direction.

1 193. Plaintiff Blount researched providers, specific health conditions and treatments,
2 looked for Defendant's locations close to her address, and scheduled doctor's appointments for
3 herself via the Defendant's Website and Account.

4 194. Plaintiff Blount also utilized Defendant's Account to refill prescriptions, look at
5 her bills and payments and to see her test results.

6 195. Plaintiff Blount has used and continues to use the same devices to maintain and
7 access an active Facebook account throughout the relevant period in this case.

8 196. Plaintiff Blount reasonably expected that her communications with Defendant via
9 the Web Properties were confidential, solely between herself and Defendant, and that such
10 communications would not be transmitted to or intercepted by a third party. However, and as a
11 result of the Meta Pixel Defendant chose to install on its Website, Plaintiff Blount's Private
12 Information was intercepted, viewed, analyzed and used by unauthorized third parties.

13 197. Defendant transmitted Plaintiff Blount's Facebook ID, computer IP address and
14 other device and unique online identifiers to Facebook. Defendant also transmitted information
15 such as health and medical information including Plaintiff's particular health condition, the type
16 of medical treatment sought, patient status and the fact that Plaintiff attempted to or did book a
17 medical appointment.

18 198. Plaintiff Blount never consented to the disclosure of or use of her Private
19 Information by third parties or to Defendant enabling third parties, including Facebook, to access
20 or interpret such information. Plaintiff Blount never consented to any third parties' receipt or
21 use of her Private Information.

22 199. Notwithstanding, through the Meta Pixel and similar technologies embedded on
23 Defendant's Web Properties, Defendant transmitted Plaintiff Blount's Private Information to, at
24 a minimum, Facebook and likely many other third parties like Google, Bing, and others.

25 200. By making these disclosures without her consent, Defendant breached Plaintiff
26 Blount's privacy and unlawfully disclosed her Private Information.

27 201. Defendant did not inform Plaintiff Blount that it had shared her Private
28 Information with Facebook.

1 202. Plaintiff Blount used and continues to use the same devices to maintain and to
2 access an active Facebook account throughout the relevant period for this case.

3 203. Plaintiff Blount has a continuing interest in ensuring that her Private Information,
4 which, upon information and belief, remains backed up in Defendant's possession, is protected
5 and safeguarded from future unauthorized disclosure(s).

6 204. Plaintiff Blount would consider using Defendant's services again and/or in greater
7 frequency if she could be assured by Defendant that the violations set forth herein were no longer
8 occurring.

9 ***Plaintiff Freriks' Experience with Banner***

10 205. As a condition of receiving Defendant's services, Plaintiff Freriks disclosed her
11 Private Information to Defendant on numerous occasions, and most recently in April 2023.

12 206. Plaintiff Freriks accessed Defendant's Website and Patient Account on her phone
13 and computer to receive healthcare services from Defendant and at Defendant's direction.

14 207. Plaintiff Freriks researched providers, specific health conditions and treatments,
15 looked for Defendant's locations close to her address, and scheduled doctor's appointments for
16 herself via the Defendant's Website and Account.

17 208. Plaintiff Freriks also utilized Defendant's Account to refill prescriptions, look at
18 her bills and payments and to see her test results.

19 209. Plaintiff Freriks has used and continues to use the same devices to maintain and
20 access an active Facebook account throughout the relevant period in this case.

21 210. Plaintiff Freriks reasonably expected that her communications with Defendant via
22 the Web Properties were confidential, solely between herself and Defendant, and that such
23 communications would not be transmitted to or intercepted by a third party. However, and as a
24 result of the Meta Pixel Defendant chose to install on its Web Properties, Plaintiff Freriks'
25 Private Information was intercepted, viewed, analyzed and used by unauthorized third parties.

26 211. Defendant transmitted Plaintiff Freriks' Facebook ID, computer IP address and
27 other device and unique online identifiers to Facebook. Defendant also transmitted information
28 such as health and medical information including Plaintiff's particular health condition, the type

1 of medical treatment sought, patient status and the fact that Plaintiffs attempted to or did book
2 a medical appointment.

3 212. Plaintiff Freriks never consented to the disclosure of or use of her Private
4 Information by third parties or to Defendant enabling third parties, including Facebook, to access
5 or interpret such information. Plaintiff Freriks never consented to any third parties' receipt or
6 use of her Private Information.

7 213. Notwithstanding, through the Meta Pixel and similar technologies embedded on
8 Defendant's Website, Defendant transmitted Plaintiff Freriks's Private Information to, at a
9 minimum, Facebook and likely many other third parties like Google, Bing, and others.

10 214. By making these disclosures without her consent, Defendant breached Plaintiff
11 Freriks's privacy and unlawfully disclosed her Private Information.

12 215. Defendant did not inform Plaintiff Freriks that it had shared her Private
13 Information with Facebook.

14 216. Plaintiff Freriks used and continues to use the same devices to maintain and to
15 access an active Facebook account throughout the relevant period for this case.

16 217. Plaintiff Freriks has a continuing interest in ensuring that her Private Information,
17 which, upon information and belief, remains backed up in Defendant's possession, is protected
18 and safeguarded from future unauthorized disclosure(s).

19 218. Plaintiff Freriks would consider using Defendant's services again and/or in greater
20 frequency if she could be assured by Defendant that the violations set forth herein were no longer
21 occurring.

22 ***Plaintiff Santiago Laboy's Experience with Banner***

23 219. As a condition of receiving Defendant's services, Plaintiff Santiago Laboy
24 disclosed her Private Information to Defendant on numerous occasions, and most recently in
25 March 2023.

26 220. Plaintiff Santiago Laboy accessed Defendant's Website and Patient Account on
27 her phone and computer to receive healthcare services from Defendant and at Defendant's
28 direction.

1 221. Plaintiff Santiago Laboy researched providers, specific health conditions and
2 treatments, looked for Defendant's locations close to her address, and scheduled doctor's
3 appointments for herself via the Defendant's Website and Account.

4 222. Plaintiff Santiago Laboy also utilized Defendant's Account to refill prescriptions,
5 look at her bills and payments and to see her test results.

6 223. Plaintiff Santiago Laboy has used and continues to use the same devices to
7 maintain and access an active Facebook account throughout the relevant period in this case.

8 224. Plaintiff Santiago Laboy reasonably expected that her communications with
9 Defendant via the Web Properties were confidential, solely between herself and Defendant, and
10 that such communications would not be transmitted to or intercepted by a third party. However,
11 and as a result of the Meta Pixel Defendant chose to install on its Web Properties, Plaintiff
12 Santiago Laboy's Private Information was intercepted, viewed, analyzed and used by
13 unauthorized third parties.

14 225. Defendant transmitted Plaintiff Santiago Laboy's Facebook ID, computer IP
15 address and other device and unique online identifiers to Facebook. Defendant also transmitted
16 information such as health and medical information including Plaintiff's particular health
17 condition, the type of medical treatment sought, patient status and the fact that Plaintiffs
18 attempted to or did book a medical appointment.

19 226. Plaintiff Santiago Laboy never consented to the disclosure of or use of her Private
20 Information by third parties or to Defendant enabling third parties, including Facebook, to access
21 or interpret such information. Plaintiff Santiago Laboy never consented to any third parties'
22 receipt or use of her Private Information.

23 227. Notwithstanding, through the Meta Pixel and similar technologies embedded on
24 Defendant's Website, Defendant transmitted Plaintiff Santiago Laboy's Private Information to,
25 at a minimum, Facebook and likely many other third parties like Google, Bing, and others.

26 228. By making these disclosures without her consent, Defendant breached Plaintiff
27 Santiago Laboy's privacy and unlawfully disclosed her Private Information.

28 229. Defendant did not inform Plaintiff Santiago Laboy that it had shared her Private

1 Information with Facebook.

2 230. Plaintiff Santiago Laboy used and continues to use the same devices to maintain
3 and to access an active Facebook account throughout the relevant period for this case.

4 231. Plaintiff Santiago Laboy has a continuing interest in ensuring that her Private
5 Information, which, upon information and belief, remains backed up in Defendant's possession,
6 is protected and safeguarded from future unauthorized disclosure(s).

7 232. Plaintiff Santiago Laboy would consider using Defendant's services again and/or
8 in greater frequency if she could be assured by Defendant that the violations set forth herein
9 were no longer occurring.

10 ***Plaintiff Jill Schreidl's Experience with Banner***

11 233. As a condition of receiving Defendant's services, Plaintiff Jill Schreidl disclosed
12 her Private Information to Defendant on numerous occasions starting in September 2022, and
13 most recently in April 2023.

14 234. Plaintiff Jill Schreidl accessed Defendant's Website and Patient Account on her
15 phone and computer to receive healthcare services from Defendant and at Defendant's direction.

16 235. Plaintiff Jill Schreidl researched providers, specific health conditions and
17 treatments, looked for Defendant's locations close to her address, and scheduled doctor's
18 appointments for herself via the Defendant's Website and Account.

19 236. Plaintiff Jill Schreidl also utilized Defendant's Account to refill prescriptions, look
20 at her bills and payments and to see her test results.

21 237. Plaintiff had surgery at Defendant's MD Anderson Cancer Center in January
22 2023.

23 238. Plaintiff Jill Schreidl has used and continues to use the same devices to maintain
24 and access an active Facebook account throughout the relevant period in this case.

25 239. Plaintiff Jill Schreidl reasonably expected that her communications with
26 Defendant via the Web Properties were confidential, solely between herself and Defendant, and
27 that such communications would not be transmitted to or intercepted by a third party.

28 240. However, and as a result of the Meta Pixel Defendant chose to install on its

1 Website, Plaintiff Jill Schreidl's Private Information was intercepted, viewed, analyzed and used
2 by unauthorized third parties.

3 241. Defendant transmitted Plaintiff Jill Schreidl's Facebook ID, computer IP address
4 and other device and unique online identifiers to Facebook. Defendant also transmitted
5 information such as health and medical information including Plaintiff's particular health
6 conditions which included results of her diagnostic mammograms, the type of medical treatment
7 sought, patient status and the fact that Plaintiff attempted to or did book a medical appointment.

8 242. Plaintiff Jill Schreidl never consented to the disclosure of or use of her Private
9 Information by third parties or to Defendant enabling third parties, including Facebook, to access
10 or interpret such information. Plaintiff Jill Schreidl never consented to any third parties' receipt
11 or use of her Private Information.

12 243. Notwithstanding, through the Meta Pixel and similar technologies embedded on
13 Defendant's Website, Defendant transmitted Plaintiff Jill Schreidl's Private Information to, at a
14 minimum, Facebook and likely many other third parties like Google, Bing and others.

15 244. By making these disclosures without her consent, Defendant breached Plaintiff
16 Jill Schreidl's privacy and unlawfully disclosed her Private Information.

17 245. Defendant did not inform Plaintiff Jill Schreidl that it had shared her Private
18 Information with Facebook.

19 246. Plaintiff Jill Schreidl is diagnosed with a specific medical condition and submitted
20 information to Defendant's Website and Account about scheduling medical appointments for
21 her condition.

22 247. Since submitting information concerning her medical diagnosis and appointments
23 to Defendant, Plaintiff Jill Schreidl began to receive unsolicited ads relating to her medical
24 condition on Facebook and Instagram.

25 248. These ads were so disconcerting to Plaintiff that she stopped using social media
26 for a period of time.

27 249. Plaintiff Jill Schreidl used and continues to use the same devices to maintain and
28 to access an active Facebook account throughout the relevant period for this case.

1 250. Plaintiff Jill Schreidl has a continuing interest in ensuring that her Private
2 Information, which, upon information and belief, remains backed up in Defendant's possession,
3 is protected and safeguarded from future unauthorized disclosure(s).

4 251. Plaintiff Jill Schreidl would consider using Defendant's services again and/or in
5 greater frequency if she could be assured by Defendant that the violations set forth herein were
6 no longer occurring.

7 ***Plaintiff John Schreidl's Experience with Banner***

8 252. As a condition of receiving Defendant's services, Plaintiff John Schreidl disclosed
9 his Private Information to Defendant on numerous occasions starting in September 2022, and
10 most recently in April 2023.

11 253. Plaintiff John Schreidl accessed Defendant's Website and Patient Account on his
12 phone and computer to receive healthcare services from Defendant and at Defendant's direction.

13 254. Plaintiff John Schreidl researched providers, specific health conditions and
14 treatments, looked for Defendant's locations close to his address, and scheduled doctor's
15 appointments for himself including imaging and surgery via the Defendant's Website and
16 Account.

17 255. Plaintiff John Schreidl also utilized Defendant's Account to refill prescriptions,
18 look at his bills and payments and to see his test results.

19 256. Plaintiff John Schreidl has used and continues to use the same devices to maintain
20 and access an active Facebook account throughout the relevant period in this case.

21 257. Plaintiff John Schreidl reasonably expected that his communications with
22 Defendant via the Web Properties were confidential, solely between herself and Defendant, and
23 that such communications would not be transmitted to or intercepted by a third party.

24 258. However, and as a result of the Meta Pixel Defendant chose to install on its
25 Website, Plaintiff John Schreidl's Private Information was intercepted, viewed, analyzed and
26 used by unauthorized third parties.

27 259. Defendant transmitted Plaintiff John Schreidl's Facebook ID, computer IP address
28 and other device and unique online identifiers to Facebook. Defendant also transmitted

1 information such as health and medical information including Plaintiff's particular health
2 conditions, the type of medical treatment sought, patient status and the fact that Plaintiff
3 attempted to or did book a medical appointment.

4 260. Plaintiff John Schreidl never consented to the disclosure of or use of his Private
5 Information by third parties or to Defendant enabling third parties, including Facebook, to access
6 or interpret such information. Plaintiff John Schreidl never consented to any third parties'
7 receipt or use of his Private Information.

8 261. Notwithstanding, through the Meta Pixel and similar technologies embedded on
9 Defendant's Website, Defendant transmitted Plaintiff John Schreidl's Private Information to, at
10 a minimum, Facebook and likely many other third parties like Google, Bing and others.

11 262. By making these disclosures without her consent, Defendant breached Plaintiff
12 John Schreidl's privacy and unlawfully disclosed his Private Information.

13 263. Defendant did not inform Plaintiff John Schreidl that it had shared his Private
14 Information with Facebook.

15 264. Plaintiff John Schreidl used and continues to use the same devices to maintain and
16 to access an active Facebook account throughout the relevant period for this case.

17 265. Plaintiff John Schreidl has a continuing interest in ensuring that his Private
18 Information, which, upon information and belief, remains backed up in Defendant's possession,
19 is protected and safeguarded from future unauthorized disclosure(s).

20 266. Plaintiff John Schreidl would consider using Defendant's services again and/or in
21 greater frequency if he could be assured by Defendant that the violations set forth herein were
22 no longer occurring.

23 TOLLING

24 267. Any applicable statute of limitations has been tolled by the "delayed discovery"
25 rule as Plaintiffs did not know (and had no way of knowing) that their Private Information was
26 unlawfully disclosed because Defendant has concealed that fact. Alternatively, applicable
27 statute of limitations has been tolled by other applicable rules or doctrines.

CLASS ACTION ALLEGATIONS

268. Plaintiffs bring this action on behalf of themselves and on behalf of various classes of persons similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure.

269. The Nationwide Class that Plaintiffs seek to represent is defined as:

All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Pixel on Defendant's Website.

270. The California Class that Plaintiff McCulley seeks to represent is defined as:

All individuals residing in the State of California whose Private Information was disclosed to a third party without authorization or consent through the Pixel on Defendant's Website.

271. The Florida Class that Plaintiff Freriks seeks to represent is defined as:

All individuals residing in the State of Florida whose Private Information was disclosed to a third party without authorization or consent through the Pixel on Defendant's Website.

272. The Colorado Class that Plaintiff Jill Schreidl and Plaintiff John Schreidl seek to represent is defined as:

All individuals residing in the State of Colorado whose Private Information was disclosed to a third party without authorization or consent through the Pixel on Defendant's Website.

273. The Nationwide Class, the California Class, the Florida Class and the Colorado Class are referred to collectively as the "Classes." Excluded from the Classes are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign and any Judge who adjudicates this case, including their staff and immediate family.

274. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

275. **Numerosity, Fed R. Civ. P. 23(a)(1).** The members of the Classes are so numerous that joinder of all of them is impracticable. Upon information and belief, there are over one million individuals whose Private Information may have been improperly accessed by Facebook. The members of each Class are ascertainable and identifiable from Defendant's

1 records.

2 276. **Commonality & Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3).** Questions
3 of law and fact common to the Classes exist and predominate over any questions affecting only
4 individual Class Members. These include:

- 5 a. Whether and to what extent Defendant has a duty to protect the PII
6 and PHI of Plaintiffs and Class Members;
- 7 b. Whether Defendant owes a duty to not disclose the PII and PHI of
8 Plaintiffs and Class Members to unauthorized third parties;
- 9 c. Whether Defendant breached its duty to protect the PII and PHI of
10 Plaintiffs and the Class Members;
- 11 d. Whether Defendant breached its duty to not disclose the PII and PHII
12 of Plaintiffs and Class Members to unauthorized third parties;
- 13 e. Whether Defendant violated its privacy policy by disclosing the PII
14 and PHI of Plaintiffs and Class Members to Facebook, Google, and/or
15 other third parties.
- 16 f. Whether Defendant adequately, promptly and accurately informed
17 Plaintiffs and Class Members that their PII and PHI would be
18 disclosed to third parties;
- 19 g. Whether Defendant violated the law by failing to promptly notify
20 Plaintiffs and Class Members that their PII and PHI had been
21 compromised;
- 22 h. Whether Defendant adequately addressed and fixed the practices
23 which permitted the disclosure of patient PHI and PII;
- 24 i. Whether Defendant engaged in unfair, unlawful or deceptive
25 practices by failing to safeguard the PII and PHI of Plaintiffs and
26 Class Members;
- 27 j. Whether Defendant violated consumer protection statutes invoked
28 herein;

- 1 k. Whether Plaintiffs and Class Members are entitled to actual,
- 2 consequential, and/or nominal damages as a result of Defendant's
- 3 wrongful conduct;
- 4 l. Whether Defendant knowingly made false representations as to its
- 5 data security and/or privacy policy practices;
- 6 m. Whether Defendant knowingly omitted material representations with
- 7 respect to its data security and/or privacy policy practices; and
- 8 n. Whether Plaintiffs and Class Members are entitled to injunctive
- 9 relief to redress the imminent and currently ongoing harm faced as a
- 10 result of Defendant's disclosure of their PII and PHI.

11 277. **Typicality, Fed. R. Civ. P. 23(a)(3).** Plaintiffs' claims are typical of those of other
 12 Class Members because all had their Private Information was compromised as a result of
 13 Defendant's use of the Meta Pixel and due to Defendant's misfeasance described herein.
 14 Plaintiffs present common claims on behalf of the absent members of the Classes that are not
 15 unique but capable of proof by applying common evidence regarding common business
 16 practices and policies to common legal theories and claims.

17 278. **Adequacy, Fed. R. Civ. P. 23(a)(4).** Plaintiffs will fairly and adequately represent
 18 and protect the interests of Class Members in that Plaintiffs have no disabling conflicts of
 19 interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief
 20 that is antagonistic or adverse to the Class Members, and the infringement of rights and the
 21 damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also
 22 retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute
 23 this action vigorously.

24 279. **Superiority and Manageability, Fed. R. Civ. P. 23(b)(3).** Class litigation is an
 25 appropriate method for fair and efficient adjudication of the claims involved. Class action
 26 treatment is superior to all other available methods for the fair and efficient adjudication of the
 27 controversy alleged herein; it will permit a large number of Class Members to prosecute their
 28 common claims in a single forum simultaneously, efficiently and without the unnecessary

1 duplication of evidence, effort and expense that hundreds of individual actions would require.
2 Class action treatment will permit the adjudication of relatively modest claims by certain Class
3 Members who could not individually afford to litigate a complex claim against a large
4 corporation, like Defendant. Further, even for those Class Members who could afford to litigate
5 such a claim, such individual actions would still be economically impractical and impose a
6 burden on the courts.

7 280. **Policies Generally Applicable to the Class.** This class action is also appropriate
8 for certification because Defendant has acted or refused to act on grounds generally applicable
9 to the Class thereby requiring the Court's imposition of uniform relief to ensure compatible
10 standards of conduct toward Class Members and making final injunctive relief appropriate with
11 respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class
12 Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendant's conduct
13 with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

14 281. The nature of this action and the nature of laws available to Plaintiffs and Class
15 Members make the use of the class action device a particularly efficient and appropriate
16 procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because
17 Defendant would otherwise gain an unconscionable advantage since it would be able to exploit
18 and overwhelm the limited resources of each individual Class Member with superior financial
19 and legal resources; the costs of individual suits could unreasonably consume the amounts that
20 would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is
21 representative of that experienced by the Class and will establish the right of each Class Member
22 to recover on the cause of action alleged; and individual actions would create a risk of
23 inconsistent results and would be unnecessary and duplicative of this litigation.

24 282. The litigation of the claims brought herein is manageable. Defendant's uniform
25 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class
26 Members demonstrate that there would be no significant manageability problems with
27 prosecuting this lawsuit as a class action.

28 283. **Ascertainability & Notice.** Membership in the Classes can be determined by

objective records maintained by Defendant and adequate notice can be given to Class Members directly using information maintained in Defendant's records.

284. **Class-wide Injunctive Relief, Fed. R. Civ. P. 23(b)(2).** Unless a Class-wide injunction is issued, Defendant may continue to fail to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint as Defendant has acted or refused to act on grounds generally applicable to the Class. Accordingly, final injunctive or corresponding declaratory relief with regard to the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure. Such relief will provide a public benefit.

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

- ◆ Whether Defendant owes a legal duty to not disclose Plaintiffs' and Class Members' Private Information;
- ◆ Whether Defendant owes a legal duty to not disclose Plaintiffs' and Class Members' Private Information under Defendant's privacy policy;
- ◆ Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- ◆ Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- ◆ Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;
- ◆ Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties; and
- ◆ Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

**ARIZONA LAW SHOULD APPLY TO PLAINTIFFS’
& CLASS MEMBERS’ COMMON LAW CLAIMS**

286. The State of Arizona has a significant interest in regulating the conduct of businesses operating within its borders.

287. Arizona, which seeks to protect the rights and interests of Arizona and all residents and citizens of the United States against a company headquartered and doing business in Arizona, has a greater interest in the claims of Plaintiffs and the Classes than any other state and is most intimately concerned with the claims and outcome of this litigation.

288. The principal place of business and headquarters of Banner, located in Phoenix, Arizona, is the “nerve center” of its business activities—the place where its high-level officers direct, control and coordinate its activities, including major policy, financial and legal decisions.

289. Upon information and good faith belief, Defendant’s actions and corporate decisions surrounding the allegations made in the Complaint were made from and in Arizona.

290. Defendant’s breaches of duty to Plaintiffs and Class Members emanated from Arizona.

291. Application of Arizona law to the Classes with respect to Plaintiffs’ and the Classes’ common law claims is neither arbitrary nor fundamentally unfair because choice of law principles applicable to this action support the application of the common law of Arizona to the nationwide common law claims of all Class members. Additionally, given Arizona’s significant interest in regulating the conduct of businesses operating within its borders, and that Arizona has the most significant relationship to Defendant, as it is headquartered in Arizona, there is no conflict in applying Arizona law to non-resident consumers such as Plaintiffs and the Class members.

292. Alternatively, and/or in addition to Arizona law, the laws set forth below apply to the conduct described herein.

CLAIMS FOR RELIEF

COUNT I

**VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT (“ECPA”)
18 U.S.C. § 2511(1), *et seq.*
Unauthorized Interception, Use and Disclosure
(By Plaintiffs on behalf of the Nationwide Class)**

293. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein and bring this claim individually and on behalf of the proposed Nationwide Class.

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

295. 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.

296. The transmissions of Plaintiffs’ PII and PHI to Defendant’s Website qualifies as a “communication” under the ECPA’s definition of 18 U.S.C. § 2510(12).

297. Electronic Communications. The transmission of PII and PHI between Plaintiffs and Class Members and Defendant’s Web Properties 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(2).

298. 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).

299. Interception. The ECPA defines an 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).

300. Electronical, Mechanical, or Other Device. The ECPA defines “electronic,

1 mechanical, or other device” as “any device ... which can be used to intercept a[n] ... electronic
2 communication[.]” 18 U.S.C. § 2510(5).

3 301. The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- 4 a. Plaintiffs’ and Class Members’ browsers;
- 5 b. Plaintiffs’ and Class Members’ computing devices;
- 6 c. Defendant’s web-servers; and,
- 7 d. The Pixel Code deployed by Defendant to effectuate sending
8 and acquiring patient communications.

9 302. By utilizing and embedding the Pixel on its Web Properties, Defendant
10 intentionally intercepted, endeavored to intercept, and/or procured another person to intercept,
11 the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. §
12 2511(1)(a).

13 303. Specifically, Defendant intercepted Plaintiffs’ and Class Members’ electronic
14 communications via the Meta Pixel, which tracked, stored, and unlawfully disclosed Plaintiffs’
15 and Class Members’ Private Information to third parties such as Facebook.

16 304. Defendant intercepted communications that include, but are not limited to,
17 communications to/from Plaintiffs and Class Members regarding PII and PHI, treatment,
18 medication, and scheduling.

19 305. By intentionally disclosing or endeavoring to disclose Plaintiffs’ and Class
20 Members’ electronic communications to affiliates and other third parties, while knowing or
21 having reason to know that the information was obtained through the interception of an
22 electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C.
23 § 2511(1)(c).

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

28 307. Unauthorized Purpose. Defendant intentionally intercepted the contents of

1 Plaintiffs' and Class Members' electronic communications for the purpose of committing a
2 tortious act in violation of the Constitution or laws of the United States or of any State – namely,
3 invasion of privacy, among others.

4 308. Defendant used the wire or electronic communications to increase its profit
5 margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class
6 Members' PII and PHI for financial gain.

7 309. Defendant was not acting under color of law to intercept Plaintiffs' and the Class
8 Members' wire or electronic communication.

9 310. Plaintiffs and Class Members did not authorize Defendant to acquire the content
10 of their communications for purposes of invading Plaintiffs' privacy via the Pixel tracking code.
11 Further, the Website Notice of Privacy Practices does not require consumers to agree to them
12 by selecting or clicking a “checkbox” presented in a sufficiently conspicuous manner to put
13 Plaintiffs on notice of them. Thus, Plaintiffs and the Class Members did not consent to
14 Defendant's use of the Pixel to track and intercept their communications with Defendant's
15 Website or other Web Properties.

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

21 312. A person who violates § 2511(1)(a) is liable for \$10,000 in statutory damages to
22 any person whose wire, oral, or electronic communication is intercepted, disclosed, or
23 intentionally used.

24 313. Defendant is liable to Plaintiffs and Class Members for violations of the ECPA.

25 314. Based on the foregoing, Plaintiffs and Nationwide Class Members seek all other
26 relief as the Court may deem just and proper, including all available monetary relief, injunctive
27 and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.
28

COUNT II

**VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(3)(a), *et seq.*
Unauthorized Divulgence by Electronic Communications Service
(By Plaintiffs on behalf of the Nationwide Class)**

315. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein and bring this claim individually and on behalf of the Nationwide Class.

316. The ECPA Wiretap statute provides that “a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.” 18 U.S.C. § 2511(3)(a).

317. Electronic Communication Service. An “electronic communication service” is defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

318. Defendant’s Web Properties are electronic communication services. The Web Properties provide Users the ability to send or receive electronic communications. In the absence of Defendant’s Web Properties, internet users could not send or receive communications regarding Plaintiffs’ and Class Members’ PII and PHI.

319. Intentional Divulgence. Defendant intentionally utilized the Meta Pixel and was, or should have been aware, that it could divulge Plaintiffs’ and Class Members’ PII and PHI.

320. While in Transmission. Divulgence of the contents of Plaintiffs’ and Class Members’ communications was contemporaneous with their exchange with Defendant’s Web Properties, to which they directed their communications.

321. Defendant divulged the contents of Plaintiffs’ and Class Members’ communications to Facebook or other third parties without Plaintiffs’ and Class Members’ consent and/or authorization.

322. Exceptions do not apply. In addition to the exception for communications directly

1 to an ECS or an agent of an ECS, the Wiretap Act states that “[a] person or entity providing
2 electronic communication service to the public may divulge the contents of any such
3 communication as follows:

- 4 a. “as otherwise authorized in section 2511(2)(a) or 2517 of this
5 title;”
- 6 b. “with the lawful consent of the originator or any addressee or
7 intended recipient of such communication;”
- 8 c. “to a person employed or authorized, or whose facilities are
9 used, to forward such communication to its destination;” or
- 10 d. “which were inadvertently obtained by the service provider
and which appear to pertain to the commission of a crime, if
such divulgence is made to a law enforcement agency.” 18
U.S.C. § 2511(3)(b).

11 323. Section 2511(2)(a)(i) provides: “It shall not be unlawful under this chapter for an
12 operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic
13 communication service, whose facilities are used in the transmission of a wire or electronic
14 communication, to intercept, disclose, or use that communication in the normal course of his
15 employment while engaged in any activity which is a necessary incident to the rendition of his
16 service or to the protection of the rights or property of the provider of that service, except that a
17 provider of wire communication service to the public shall not utilize service observing or
18 random monitoring except for mechanical or service quality control checks.”

19 324. Defendant’s divulgence of the contents of Plaintiffs’ and Class Members’
20 communications on Defendant’s Web Properties to a third party was not authorized by 18 U.S.C.
21 § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant’s
22 service; nor (2) necessary to the protection of the rights or property of Defendant.

23 325. Defendant’s divulgence of the contents of user communications on Defendant’s
24 browser through the Pixel code was not done “with the lawful consent of the originator or any
25 addresses or intended recipient of such communication[s].” As alleged above: (a) Plaintiffs and
26 Class Members did not authorize Defendant to divulge the contents of their communications;
27 and (b) Defendant did not procure the “lawful consent” from the Websites or apps with which
28 Plaintiffs and Class Members were exchanging information.

326. Moreover, Defendant divulged the contents of Plaintiffs' and Class Members' communications through the Meta Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

327. The contents of Plaintiffs' and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

328. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; and reasonable attorneys' fees and other litigation costs reasonably incurred.

329. A person who violates § 2511(3)(a) is liable for \$10,000 in statutory damages to any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used.

330. Defendant is liable to Plaintiffs and Class Members for violations of the ECPA.

331. Based on the foregoing, Plaintiffs and Nationwide Class Members seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

COUNT III

VIOLATION OF ARIZONA CONSUMER FRAUD ACT A.R.S. §44-1521 *et seq.* (On behalf of Plaintiffs & the Nationwide Class)

332. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein and bring this claim individually and on behalf of the Nationwide Class.

333. The Arizona Consumer Fraud Act, A.R.S. 44-1521 *et seq.*, prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of Arizona.

334. A.R.S. § 44-1522 provides in pertinent part:

(a) The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission

of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice.. By the acts and conduct alleged herein, Defendant was selling or advertising merchandise as those terms are defined in A.R.S. § 44-1521.

335. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices in and from Arizona, in violation of the Arizona Consumer Fraud Act, by:

- a. promising to maintain the privacy and security of Plaintiffs' and Class Members' protected health information as required by law;
- b. installing the Meta Pixel to operate as intended and transmit Plaintiffs' and Class Members' Private Information without their authorization to Facebook;
- c. failing to disclose or omitting material facts to Plaintiffs and Class Members regarding the disclosure of their Private Information to Facebook;
- d. failing to take proper action to ensure the Pixel was configured to prevent unlawful disclosure of Plaintiffs' and Class Members' Private Information;
- e. unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook;
- f. Deceptively representing to Plaintiff and Class Members that it did not use Pixel when it did.

336. Defendant knew or should have known that its conduct was of the nature prohibited by A.R.S. § 44-1522, *et seq.*

337. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant knew it failed to disclose to Plaintiffs and Class Members that their healthcare related communications via the Web Properties would be disclosed to Facebook.

338. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant intended that Plaintiffs and Class Members rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods, merchandise and services.

339. Specifically, Defendant was aware that Plaintiffs and Class Members depended and relied upon it to keep their communications confidential and Defendant instead disclosed

1 that information to Facebook.

2 340. Contrary to its duties as a medical provider and its express promises of
3 confidentiality, Defendant deployed the Pixel to disclose and transmit Plaintiffs' personally
4 identifiable, non-public medical information, and the contents of her communications
5 exchanged with Defendant to third parties, *i.e.*, Facebook.

6 341. Defendant's disclosures of Plaintiffs' and Class Members' Private Information
7 were made without their knowledge, consent, or authorization, and were unprivileged.

8 342. The harm arising from a breach of provider-patient confidentiality includes
9 erosion of the essential confidential relationship between the healthcare provider and the patient.

10 343. Defendant willfully, knowingly, intentionally, and voluntarily engaged in the
11 aforementioned acts when it incorporated the Meta Pixel on its Web Properties, with knowledge
12 of the Pixel's purpose and functionality, and further utilized the benefits that Pixel provides
13 website owners to the detriment of Plaintiffs and the Nationwide Class Members.

14 344. Plaintiffs and the Nationwide Class Members could not have avoided the harms
15 described herein through the exercise of ordinary diligence.

16 345. Defendant also had a duty to disclose the material information that Plaintiffs and
17 Nationwide Class Members' Private Information was being shared with a third party as, among
18 other things: a) Defendant had superior knowledge of such facts and Plaintiffs and Nationwide
19 Class Members had no other way to obtain the information; b) by reason of its status as a
20 provider of medical and mental healthcare services, Defendant was in a special relationship with
21 Plaintiffs and Nationwide Class Members—Medical providers have a duty (defined by HIPAA
22 and other federal and state laws and regulations) to keep patients' non-public medical
23 information completely confidential; c) the facts not disclosed relate to health and safety of
24 Plaintiff and Nationwide Class Members; d) Defendant made certain affirmative statements
25 regarding its privacy policy but failed to disclose all material facts (including that it was sharing
26 Private Information with third-parties, and not using Pixels, as described herein) making its
27 partial disclosures misleading, confusing and deceptive to reasonable consumers in the
28 Nationwide Class.

1
2 346. As a result of Defendant's actions, Plaintiffs and Nationwide Class Members have
3 suffered harm and injury.

4 347. Defendant's unlawful conduct is ongoing. Thus, Injunctive and declaratory relief
5 is necessary and appropriate to prevent further violations.

6 348. Plaintiffs and Nationwide Class Members have been damaged as a direct and
7 proximate result of Defendant's invasion of their privacy and are entitled to just compensation,
8 including monetary damages.

9 349. Plaintiffs and Nationwide Class Members seek appropriate relief for these injuries,
10 including but not limited to damages that will reasonably compensate Plaintiffs and Nationwide
11 Class Members for the harm to their privacy interests as a result of Defendant's violation of the
12 Arizona Consumer Fraud Act.

13 350. Plaintiffs and Nationwide Class Members seek all other relief as the Court may
14 deem just and proper, including all available monetary relief, injunctive and declaratory relief,
15 any applicable penalties, and reasonable attorneys' fees and costs.

16
17 **COUNT IV**

18 **COMMON LAW INVASION OF PRIVACY – INTRUSION UPON SECLUSION**
19 **(By Plaintiffs on behalf of the Nationwide Class)**

20 351. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully
21 set forth herein and bring this claim individually and on behalf of the Nationwide Class.

22 352. Plaintiffs and Nationwide Class Members had a reasonable expectation of privacy
23 in their communications with Defendant via its Website and the communication platforms and
24 services therein.

25 353. Plaintiffs and Nationwide Class Members communicated sensitive and protected
26 medical information and individually identifiable information that they intended for only
27 Defendant to receive and that they understood and expected Defendant would keep private.

28 354. Defendant's disclosure of the substance and nature of those communications to

1 third parties without the knowledge and consent of Plaintiffs and Nationwide Class Members is
2 an intrusion on Plaintiffs' and Nationwide Class Members' solitude or seclusion.

3 355. Plaintiffs and Nationwide Class Members had a reasonable expectation of privacy
4 because Defendant's Web Notice of Privacy Practices states that they can expect such privacy.

5 356. Moreover, Plaintiffs and Nationwide Class Members have a general expectation
6 that their communications regarding healthcare with their healthcare providers will be kept
7 confidential.

8 357. Defendant's disclosure of private medical information coupled with individually
9 identifying information is highly offensive to the reasonable person.

10 358. As a result of Defendant's actions, Plaintiffs and Nationwide Class Members have
11 suffered harm and injury, including but not limited to an invasion of their privacy rights.

12 359. Plaintiffs and Nationwide Class Members have been damaged as a direct and
13 proximate result of Defendant's invasion of their privacy and are entitled to just compensation,
14 including monetary damages.

15 360. Based on the foregoing, Plaintiffs and Nationwide Class Members seek
16 appropriate relief for these injuries, including but not limited to damages that will reasonably
17 compensate Plaintiffs and Nationwide Class Members for the harm to their privacy interests as
18 a result of the intrusion(s) upon Plaintiffs' and Nationwide Class Members' privacy.

19 361. Based on the foregoing, Plaintiffs and Nationwide Class Members seek all other
20 relief as the Court may deem just and proper.

21 **COUNT V**

22 **BREACH OF CONFIDENCE**

23 **(By Plaintiffs on behalf of the Nationwide Class)**

24 362. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully
25 set forth herein and bring this claim individually and on behalf of the Nationwide Class.

26 363. Medical providers have a duty to keep patients' non-public medical information
27 completely confidential.

28 364. Plaintiffs and Nationwide Class Members had reasonable expectations of privacy

1 in their communications exchanged with Defendant, including communications exchanged on
 2 Defendant's Website, because Defendant is in the business of providing medical and mental
 3 health care.

4 365. Plaintiffs' and Nationwide Class Members' reasonable expectations of privacy in
 5 the communications exchanged with Defendant are further supported by Defendant's express
 6 promises in its Privacy Policies.

7 366. In breach of its duties as a medical provider and its express promises of
 8 confidentiality, Defendant deployed the Meta Pixel to disclose and transmit Plaintiffs' and
 9 Nationwide Class Members' Private Information and the contents of private healthcare
 10 communications exchanged with Defendant to third parties, including Facebook.

11 367. Defendant's disclosures of Plaintiffs' and Nationwide Class Members' Private
 12 Information were made without their knowledge, consent or authorization.

13 368. As a direct result of Defendant's breach of provider-patient confidentiality,
 14 Defendant eroded the essential confidential relationship between a healthcare provider and
 15 patient.

16 369. As a direct and proximate cause of Defendant's unauthorized disclosures of
 17 patients' personally identifiable, non-public medical information and communications,
 18 Plaintiffs and Nationwide Class members were damaged, including the following:

- 19 a. Sensitive and confidential information that Plaintiffs and
 20 Nationwide Class Members intended to remain private is no
 longer private;
- 21 b. Defendant eroded the essential confidential nature of the
 22 provider-patient relationship;
- 23 c. Defendant took something of value from Plaintiffs and
 24 Nationwide Class Members and derived benefit therefrom
 25 without Plaintiffs' and Nationwide Class Members'
 knowledge or informed consent and without compensating
 Plaintiffs and Nationwide Class Members for the data;
- 26 d. Plaintiffs and Nationwide Class Members did not get the full
 27 value of the medical services for which they paid, which
 included Defendant's duty to maintain confidentiality;
- 28 e. Defendant's actions diminished the value of Plaintiffs' and
 Nationwide Class Members' Private Information and

f. Defendant's actions violated the property rights Plaintiffs and Nationwide Class Members have in their Private Information.

370. Based on the foregoing, Plaintiffs and Nationwide Class Members are therefore entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation.

COUNT VI

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA")

Cal. Penal Code §§ 630, *et seq.*

(By Plaintiff McCulley on Behalf of the California Class)

371. Plaintiff McCulley repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the California Class.

372. The California Invasion of Privacy Act ("CIPA") is codified at California Penal Code §§ 630 to 638.

373. CIPA represents a fundamental policy of the state of California which cannot be waived or contracted out of.

374. CIPA begins with its statement of purpose.

The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

CAL. PENAL CODE § 630.

375. California Penal Code § 631(a) provides, in pertinent part:

Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, 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, is punishable by a fine not exceeding two thousand five hundred dollars (\$2,500)[.]

1 376. Simply put, a defendant must show it had the consent of *all* parties to a
2 communication before it can record any portion of that communication.

3 377. At all relevant times, Defendant has been a person that CIPA applies. Cal. Penal
4 Code §631(a).

5 378. At all relevant times, Defendant aided, employed, agreed with, and conspired with
6 Facebook to track and intercept Plaintiff's and the California Class Members' internet
7 communications while using Defendant's Web Properties.

8 379. These communications were intercepted by a third party during the
9 communications and without the knowledge, authorization or consent of Plaintiff and California
10 Class Members.

11 380. Defendant intentionally inserted an electronic device (the Pixel) that, without the
12 knowledge and consent of Plaintiff and Class members, recorded and transmitted their
13 confidential communications with Defendant to a third party.

14 381. Defendant willingly facilitated and aided Facebook's interception and collection
15 of Plaintiff's and California Class Members' Private Information by embedding the Pixel(s) on
16 the Web Properties, thereby assisting Facebook's eavesdropping.

17 382. The following items constitute "machine[s], instrument[s], or contrivance[s]"
18 under the CIPA, and even if they do not, the Pixel falls under the broad catch-all category of
19 "any other manner":

- 20 a. The computer codes and programs Facebook used to track
21 Plaintiff's and California Class Members' communications
 while they were navigating the Web Properties;
- 22 b. Plaintiff's and California Class Members' browsers;
- 23 c. Plaintiff's and California Class Members' computing and
24 mobile devices;
- 25 d. Facebook's web and ad servers;
- 26 e. The web and ad servers from which Facebook tracked and
27 intercepted Plaintiff's and California Class Members'
 communications while they were using a web browser to
 access or navigate the Web Properties;
- 28 f. The computer codes and programs used by Facebook to

effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit the Web Properties; and

- g. The plan Facebook carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser or mobile application to visit the Web Properties.

383. Defendant fails to disclose to Users that it is using the Pixel to track and automatically and simultaneously transmit highly sensitive personal communications to a third party, and in fact, expressly disavows using the Pixel on its Website.⁵⁹ Defendant is necessarily aware that these communications are confidential as its Website Notice of Privacy Practices acknowledges the confidential nature of private medical information and disclaims that it is being shared with unidentified third parties without Plaintiff's and California Class Members' express authorization. Thus, Defendant is acting in intentional violation of Plaintiff's privacy.

384. The patient communication information that Defendant transmits while using the Pixel constitutes protected health information.

385. As demonstrated herein, Defendant violates CIPA by aiding and permitting third parties to receive its patients' online communications in real time through its Web Properties without their consent.

386. By choosing to install the Pixel and disclosing Plaintiff's and California Class Members' private health information, Defendant violated Plaintiff's and California Class Members' statutorily protected right to privacy.

387. As a result of the above violations and pursuant to CIPA Section 637.2, Defendant is liable to Plaintiff and California Class Members for the greater of: a) treble actual damages related to their loss of privacy in an amount to be determined at trial; or b) for statutory damages in the amount of \$5,000 per violation. Penal Code § 637.2 specifically states that "[i]t is not a necessary prerequisite to an action pursuant to this section that the Plaintiff has suffered, or be threatened with, actual damages."

⁵⁹ <https://www.bannerhealth.com/about/legal-notices/privacy> ("**Information Collected Using Pixel Tags or Clear GIFs.** Pixel Tags or Clear GIFs, also known as Web Beacons or Web Bugs, are transparent graphical images placed on a website. Currently, Banner Health does not use them on its site.")

388. Under the statute, Defendant is also liable for reasonable attorney's fees, litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

389. Based on the foregoing, Plaintiff and California Class Members seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

COUNT VII

VIOLATION OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA")

Cal. Civ. Code §§ 56, *et seq.*

(By Plaintiff McCulley on behalf of the California Class)

390. Plaintiff McCulley repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the California Class.

391. The California Confidentiality of Medical Information Act, California Civil Code §§ 56, *et seq.* ("CMIA") prohibits health care providers from disclosing medical information relating to their patients without patient authorization.

392. "Medical information" refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care . . . regarding a patient's medical history, mental or physical condition, or treatment. 'Individually Identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual[.]" Cal. Civ. Code § 56.05.

393. The CMIA applies to Defendant in all regards. Defendant is a business under Cal. Civil Code §56.06 and therefore, is subject to the requirements of the CMIA, including but not limited to §§56.10 and 56.101.

394. Defendant is a "provider of health care" as defined by California Civil Code § 56.06(b).

395. Plaintiff and California Class Members are patients, and, as a health care provider,

1 Defendant has an ongoing obligation to comply with the CMIA's requirements.

2 396. Cal. Civil Code § 56.10 states, in pertinent part, that "[n]o provider of health care
3 . . . shall disclose medical information regarding a patient of the provider of health care . . .
4 without first obtaining an authorization" Section 56.101 of the CMIA states, in pertinent
5 part, that "[a]ny provider of health care . . . or contractor . . . who negligently creates, maintains,
6 preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the
7 remedies and penalties" Cal. Civ. Code §§ 56.10, 56.101. Through the conduct described
8 herein, Defendant violated the CMIA, including these sections.

9 397. As set forth above, device identifiers, web URLs, Internet Protocol (IP) addresses
10 and other characteristics that can uniquely identify Plaintiff McCulley and California Class
11 Members are transmitted to Defendant in combination with patient medical conditions, medical
12 concerns, treatment(s) sought by the patients, medical history and other medical information.
13 This is protected health information under the CMIA.

14 398. This private medical information is intercepted and transmitted to Facebook via
15 Defendant's use of the Pixel and other enabling software on its Website. Facebook ID is also an
16 identifier sufficient to allow identification of an individual. Along with patients' Facebook ID,
17 Defendant discloses to Facebook several pieces of information regarding patients' use of its
18 Web Properties, including but not limited to the following: patient medical conditions, medical
19 concerns, treatment(s) sought by the patients, medical specialty of the doctor(s) searched for and
20 selected by patients and appointment information.

21 399. Upon information and belief, the private medical information of Plaintiff
22 McCulley and California Class Members that was improperly intercepted and transmitted to
23 Facebook via Defendant's use of the Pixel was subsequently improperly viewed, accessed, acted
24 upon and otherwise used by Facebook to, among other things, tailor advertisements to them
25 based on their medical conditions and other private medical information for gain.

26 400. The information described above constitutes medical information pursuant to the
27 CMIA because it is patient information derived from a provider of health care regarding
28 patients' medical treatment and physical condition, and this medical information is linked with

1 individually identifying information. *See* CAL. CIV. CODE § 56.05(i).

2 401. As demonstrated herein, Defendant fails to obtain its patients' authorization for
3 the disclosure of medical information and fails to disclose in its Privacy Policy⁶⁰ that it shares
4 protected health information with Facebook or other third parties for marketing purposes.

5 402. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical
6 information must be:

- 7 (1) Clearly separate from any other language present on the same page and is executed
- 8 by a signature which serves no other purpose than to execute the authorization;
- 9 (2) signed and dated by the patient or her representative;
- 10 (3) state the name and function of the third party that receives the information; and
- (4) state a specific date after which the authorization expires.

11 CMIA Section 56.11. Further, the Website Notice of Privacy Practices does not require
12 consumers to agree to them by selecting or clicking a "checkbox" presented in a sufficiently
13 conspicuous manner to put Plaintiffs on notice of them. Accordingly, the information set forth
14 in Defendant's Website Privacy Notice does not qualify as a valid authorization.

15 403. As described above, Defendant is intentionally violating the CMIA by choosing
16 to install the Pixel and disclosing its patients' medical information to Facebook along with the
17 patients' individually identifying information. Accordingly, Plaintiff and California Class
18 Members seek all relief available for Defendant's CMIA violations.

19 404. Based on the foregoing, Plaintiff and California Class Members seek nominal
20 damages, compensatory damages, punitive damages, attorneys' fees and costs of litigation for
21 Defendant's violation(s) of the CMIA.

22
23
24
25
26
27 ⁶⁰ <https://www.bannerhealth.com/about/legal-notices/privacy> (last visited May 29, 2023);
28 <https://www.bannerhealth.com/-/media/files/project/bh/patients-visitors/privacy-practices/hipaa-eng-fs-03-28-19.ashx> (last visited May 29, 2023)

COUNT VIII

**VIOLATION OF THE UNFAIR COMPETITION LAW (“UCL”)
Cal. Bus. & Prof. Code § 17200, *et seq.* – Unlawful Business Practices
(By Plaintiff McCulley on behalf of the California Class)**

405. Plaintiff McCulley repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the California Class.

406. Plaintiff McCulley, California Class Members and Defendant are each a “person” under Cal. Bus. & Prof. Code § 17201.

407. The acts, omissions and conduct of Defendant as alleged herein constitute “business practices” within the meaning of the UCL.

408. California Business and Professions Code §§ 17201, *et seq.*, prohibits acts of unfair competition, which includes unlawful business practices.

409. Plaintiff McCulley brings her claim for injunctive relief as she has no confidence that Defendant has altered its privacy practices and she may wish to use Defendant’s services in the future.

410. Plaintiff McCulley brings her claim for restitution in the alternative to her claims for damages.

411. Defendant engaged in unlawful business practices by disclosing Plaintiff McCulley’s and California Class Members’ Private Information to unrelated third parties, including Facebook, without prior consent in violation of the consumer protection and privacy statutes alleged herein.

412. Defendant’s unlawful acts and practices include violations of Plaintiff McCulley’s and Class Member’s constitutional rights to privacy; Cal. Penal Code §§ 630, *et seq.*; Cal. Civ. Code §§ 56, *et seq.*; 18 U.S.C. § 2511(1), *et seq.*; 18 U.S.C. § 2511(3)(a), *et seq.*; and 18 U.S.C. § 1030, *et seq.*

413. Because Defendant is in the business of providing medical and mental healthcare services, Plaintiff McCulley and California Class Members relied on Defendant to advise them of any potential disclosure of their private information.

1 414. Plaintiff McCulley and California Class Members were entitled to assume (and
2 did assume) that Defendant would take appropriate measures to keep their private information
3 private and confidential.

4 415. Plaintiff McCulley and the California Class Members reasonably relied upon the
5 representations Defendant made in its Privacy Policy, including those representations
6 concerning the confidentiality of patient information.

7 416. Defendant's failure to disclose that it was sharing Private Information with third
8 parties constitutes a material omission of fact. Additionally, Defendant's express representation
9 that it was not using Pixels on its Website is false and misleading to Defendant's patients and
10 members of the Class.

11 417. Defendant was in sole possession of and had a duty to disclose the material
12 information that Plaintiff McCulley's and California Class Members' Private Information was
13 being shared with a third party.

14 418. Defendant also had a duty to disclose the material information that Plaintiff
15 McCulley's and California Class Members' Private Information was being shared with a third
16 party as: a) Defendant had superior knowledge of such facts and Plaintiff McCulley and
17 California Class Members had no other way to obtain the information; b) by reason of its status
18 as a provider of medical and mental healthcare services, Defendant was in a special relationship
19 with Plaintiff McCulley and California Class Members—Medical providers have a duty
20 (defined by HIPAA and other federal and state laws and regulations) to keep patients' non-
21 public medical information completely confidential; c) the facts not disclosed relate to health
22 and safety of Plaintiff McCulley and California Class Members; d) Defendant made certain
23 affirmative statements regarding its privacy policy but failed to disclose all material facts
24 (including that it was sharing Private Information with third-parties, and not using Pixels, as
25 described herein) making its partial disclosures misleading, confusing and deceptive to
26 reasonable consumers in the California Class.

27 419. Had Defendant disclosed that it shared Private Information with third parties,
28 Plaintiff McCulley would not have used Defendant's services at the level she did or would have

1 paid considerably less for those services. As a result, Plaintiff suffered injury and out of pocket
2 loss.

3 420. The harm caused by Defendant's conduct outweighs any potential benefits
4 attributable to such conduct and there were reasonably available alternatives to further
5 Defendant's legitimate business interests other than the conduct described herein.

6 421. As a direct result of their reliance on Defendant's representations that it would
7 keep personal information confidential, Plaintiff and California Class Members shared highly
8 sensitive information through their use of the Web Properties, causing them to suffer injury and
9 loss when Defendant disclosed that information to a third party.

10 422. Plaintiff McCulley requests appropriate injunctive and declaratory relief against
11 the continuation of the practices described and complained of herein. Such relief will create a
12 public benefit. Plaintiff McCulley separately seeks public injunctive relief on behalf of the
13 general public of California who have yet to deal with Defendant in the manner described herein,
14 but are likely to in the future, and therefore, are in need of protection provided by the public
15 injunctive relief sought. Such public injunctive relief will create additional public benefits.

16 423. As a direct result of Defendant's violations of the UCL, Plaintiff McCulley and
17 California Class Members have suffered injury in fact and lost money or property including, but
18 not limited to, payments to Defendant and/or other valuable consideration, such as access to
19 their private and personal data. The unauthorized access to Plaintiff McCulley's and California
20 Class Members' private and personal data also diminished the value of that information.

21 424. As a direct result of its unlawful practices, Defendant has been unjustly enriched
22 and should be required to make restitution to Plaintiff McCulley and California Class Members
23 pursuant to §§ 17203 and 17204 of the California Business & Professions Code, disgorgement
24 of all profits accruing to Defendant because of its unlawful business practices, declaratory relief,
25 attorney's fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5) and injunctive or other
26 equitable relief.

COUNT IX

**VIOLATION OF THE UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, *et seq.* – Unfair Prong
(By Plaintiff McCulley on behalf of the California Class)**

425. Plaintiff McCulley repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the California Class.

426. Defendant engaged in unfair business practices by disclosing Plaintiff McCulley's and California Class Members' Private Information to unrelated third parties, including Facebook, without prior consent despite its promises to keep such information confidential.

427. Defendant's unfair business practices included widespread violations of Plaintiff McCulley's and California Class Members' rights to privacy, including its failure to inform the public that using its Web Properties would result in disclosing very private information to a third party.

428. Because Defendant is in the business of providing medical and mental healthcare services, McCulley and California Class Members relied on Defendant to advise them of any potential disclosure of their Private Information.

429. Plaintiff McCulley and California Class Members were entitled to assume, and did assume, that Defendant would take appropriate measures to keep their Private Information secure and confidential.

430. Plaintiff McCulley and the California Class Members reasonably relied upon the representations Defendant made in its Privacy Policy, including those representations concerning the confidentiality of patient information.

431. Defendant was in sole possession of and had a duty to disclose the material information that Plaintiff McCulley's and Class Members' private information was being shared with a third party.

432. Had Defendant disclosed that it shared Private Information with third parties, Plaintiff McCulley and the California Class would not have used Defendant's services at the level she did or would have paid considerably less for those services.

1 433. The harm caused by the Defendant's conduct outweighs any potential benefits
2 attributable to such conduct and there were reasonably available alternatives to further
3 Defendant's legitimate business interests other than Defendant's conduct described herein.

4 434. Defendant's acts, omissions and conduct also violate the unfair prong of the UCL
5 because those acts, omissions and conduct offended public policy (including the aforementioned
6 federal and state privacy statutes and state consumer protection statutes, such as HIPAA and
7 CIPA, the ECPA, and CFAA, and constitute immoral, unethical, oppressive, and unscrupulous
8 activities that caused substantial injury, including to Plaintiff McCulley and California Class
9 Members.

10 435. As a direct result of their reliance on Defendant's representations that it would
11 keep personal information confidential and Defendant's express representation that it did not
12 use Pixel on its Website, Plaintiff McCulley and California Class Members shared highly
13 sensitive information through their use of the Web Properties, causing them to suffer damages
14 when Defendant disclosed that information to a third party.

15 436. As a direct result of Defendant's violations of the UCL, Plaintiff McCulley and
16 California Class Members have suffered injury in fact and lost money or property, including but
17 not limited to payments to Defendant and/or other valuable consideration. The unauthorized
18 access to Plaintiff McCulley's and California Class Members' private and personal data also
19 diminished the value of that information.

20 437. As a direct result of its unfair practices, Defendant has been unjustly enriched and
21 should be required to make restitution to Plaintiff McCulley and California Class Members
22 pursuant to §§ 17203 and 17204 of the California Business & Professions Code, disgorgement
23 of all profits accruing to Defendant because of its unlawful business practices, declaratory relief,
24 attorney's fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5) and injunctive or other
25 equitable relief.

COUNT X**VIOLATION OF FLORIDA SECURITY OF COMMUNICATIONS ACT (“FSCA”)****Fla. Stat. 934.01 *et seq.*****(On behalf of Plaintiff Freriks & the Florida Class)**

438. Plaintiff Freriks repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the Florida Class.

439. Where there is a reasonable expectation of privacy, absent the consent of all parties, the FSCA prohibits, among other things the intentional interception or procurement of another person to intercept any wire, oral or electronic communication. Fla. Stat. §§ 934.03(1), 934.03(2)(d).

440. Any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, a wire, electronic or oral communication in violation of the FSCA is subject to a civil action for, among other things: (a) actual damages, not less than liquidated damages computed at the rate of \$100/day for each violation or \$1,000, whichever is higher; (b) punitive damages; and (c) reasonable attorneys’ fees and other litigation costs reasonably incurred. Fla. Stat. § 934.10.

441. Under the FSCA, “intercept” is defined as the “[a]ural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” Fla. Stat. § 934.02(3).

442. Under the FSCA, “contents” in the context of “any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.” Fla. Stat. § 934.02(7).

443. Under the FSCA, “person” is defined as, inter alia, “any individual, partnership, association, joint stock company, trust, or corporation.” Fla. Stat. § 934.02(5).

444. With some exclusions that do not impact Plaintiff’s claims, under the FSCA, “electronic communication” is defined as “[a]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system that affects intrastate, interstate, or foreign commerce” Fla. Stat. 934.02(12).

1 445. The Florida Security of Communications Act (“FSCA”) prohibits: (1) the
2 interception or procurement of another to intercept any wire, oral or electronic communication;
3 (2) the intentional disclosure of the contents of any wire, oral or electronic communication that
4 the discloser knew or should have known was obtained through the interception of a wire, oral
5 or electronic communication; and (3) the intentional use of the contents of any wire, oral or
6 electronic communication that the discloser knew or should have known was obtained through
7 the interception of a wire, oral or electronic communication. Fla. Stat. 934.03(1).

8 446. Any person who intercepts, discloses or uses or procures any other person to
9 intercept, disclose or use, a wire, oral or electronic communication in violation of the FSCA is
10 subject to a civil action for: (1) actual damages, not less than liquidated damages computed at
11 a rate of \$100 per day for each violation or \$1,000, whichever is higher; (2) punitive damages;
12 and (3) reasonable attorneys’ fees and other litigation costs incurred. Fla. Stat. 934.10.

13 447. At all relevant times, Defendant procured Facebook to contemporaneously track
14 and intercept Plaintiff’s and Florida Class Members’ internet communications while navigating
15 the Web Properties.

16 448. Defendant procured Facebook to contemporaneously intercept these
17 communications without authorization and consent from Plaintiff Freriks and Florida Class
18 members.

19 449. Defendant, when procuring Facebook to intercept Plaintiff Freriks’s and Florida
20 Class Members’ communications, intended Facebook to contemporaneously learn the meaning
21 of the content of Plaintiff Freriks’s and Florida Class Members’ communications with
22 Defendant.

23 450. Plaintiff Freriks and Florida Class Members had a justified and reasonable
24 expectation under the circumstances that their electronic communications would not be
25 intercepted.

26 451. Plaintiff Freriks and Florida Class Members were not aware that their electronic
27 communications were being intercepted by Facebook and did not consent to the interception.

28 452. In connection with procuring Facebook’s contemporaneous interception of

1 Plaintiff Freriks's and Florida Class Members' communications with Defendant, Defendant
2 embedded the Facebook Tracking Pixel on the Web Properties.

3 453. The Facebook Tracking Pixel constitutes an electronic or other device through
4 which the contents of a wire, oral and electronic communication can be acquired, including the
5 contents of Plaintiff Freriks's and Florida Class Members' communications with Defendant
6 via the Web Properties.

7 454. Defendant's disclosures of Plaintiffs' and Class Members' Private Information
8 were made without their knowledge, consent, or authorization, and were unprivileged.

9 455. The harm arising from a breach of provider-patient confidentiality includes
10 erosion of the essential confidential relationship between the healthcare provider and the patient.

11 456. Defendant willfully, knowingly, intentionally, and voluntarily engaged in the
12 aforementioned acts when it incorporated the Meta Pixel on its Web Properties, with knowledge
13 of the Pixel's purpose and functionality, and further utilized the benefits that Pixel provides
14 website owners to the detriment of Plaintiff Freriks and the Florida Class Members.

15 457. Plaintiff Freriks and the Florida Class Members could not have avoided the harms
16 described herein through the exercise of ordinary diligence.

17 458. As a result of Defendant's actions, Plaintiff Freriks and Florida Class Members
18 have suffered harm and injury.

19 459. Defendant's unlawful conduct is ongoing. Thus, injunctive and declaratory relief
20 is necessary and appropriate to prevent further violations.

21 460. Plaintiff Frerisk and Florida Class Members have been damaged as a direct and
22 proximate result of Defendant's invasion of their privacy and are entitled to just compensation,
23 including monetary damages.

24 461. Plaintiff Freriks and the Florida Class Members seek appropriate relief for these
25 injuries, including but not limited to damages that will reasonably compensate them for the harm
26 to their privacy interests as a result of Defendant's violation of the Florida Security of
27 Communications Act.

28 462. Plaintiff Freriks and Florida Class Members seek all other relief as the Court may

1 deem just and proper, including all available monetary relief, injunctive and declaratory relief,
 2 any applicable penalties, and reasonable attorneys' fees and costs.

3 4 **COUNT XI**

5 **VIOLATION OF THE COLORADO CONSUMER PROTECTION ACT** 6 **Colo. Rev. Stat. Section 6-1-101 *et seq.*** 7 **(On behalf of Plaintiffs Jill and John Schreidl & the Colorado Class)**

8 463. Plaintiffs Jill and John Schreidl repeat the allegations contained in the foregoing
 9 paragraphs as if fully set forth herein and bring this claim individually and on behalf of the
 10 Colorado Class.

11 464. The Colorado Consumer Protection Act, Colo. Rev. Stat. Section 6-1-101 *et seq.*
 12 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in
 13 the furnishing of any service in the state of Colorado.

14 465. Plaintiff and the members of the Colorado Class may maintain claims under the
 15 Colorado Consumer Protection Act pursuant to Colo. Rev. Stat. Section 6-1-113 and seek
 16 damages, restitution, injunctive relief, reasonable attorneys' fees and costs and other relief that
 17 may be just and equitable in the circumstances. Plaintiffs Jill and John Schreidl and members of
 18 the Colorado Class are (a) actual or potential consumer of Defendant's goods, services, or
 19 property and have been injured as a result of Defendant's deceptive trade practices; or (b) are
 20 successors in interest to an actual consumer who purchased the defendant's goods, services, or
 21 property; or (c) In the course of their person's business or occupation, were injured as a result of
 22 Defendant's deceptive trade practice.

23 466. The Colorado Consumer Protection Act pursuant to Colo. Rev. Stat. Section 6-1-
 24 105, prohibits, deceptive trade practices, including but not limited to:

25 (b) Either knowingly or recklessly makes a false representation as to the source,
 26 sponsorship, approval, or certification of goods, services, or property;

27 (c) Either knowingly or recklessly makes a false representation as to affiliation,
 28 connection, or association with or certification by another;

(e) Either knowingly or recklessly makes a false representation as to the characteristics, ingredients, uses, benefits, alterations, or quantities of goods, food, services, or property or a false representation as to the sponsorship, approval, status, affiliation, or connection of a person therewith;

(g) Represents that goods, food, services, or property are of a particular standard, quality, or grade, or that goods are of a particular style or model, if he knows or should know that they are of another;

(i) Advertises goods, services, or property with intent not to sell them as advertised;

(u) Fails to disclose material information concerning goods, services, or property which information was known at the time of an advertisement or sale if such failure to disclose such information was intended to induce the consumer to enter into a transaction;

(rrr) Either knowingly or recklessly engages in any unfair, unconscionable, deceptive, deliberately misleading, false, or fraudulent act or practice.

467. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices in violation of the Colorado Consumer Protection Act, by:

a. promising to maintain the privacy and security of Plaintiffs Jill and John Schreidl's and Colorado Class Members' protected health information as required by law;

b. installing the Meta Pixel to operate as intended and transmit Plaintiffs Jill and John Schreidl's and Colorado Class Members' Private Information without their authorization to Facebook;

c. failing to disclose or omitting material facts to Plaintiffs Jill and John Schreidl and Colorado Class Members regarding the disclosure of their Private Information to Facebook;

d. failing to take proper action to ensure the Pixel was configured to prevent unlawful disclosure of Plaintiffs Jill and John Schreidl's and Colorado Class Members' Private Information;

e. unlawfully disclosing Plaintiffs Jill and John Schreidl's and Colorado Class Members' Private Information to Facebook;

f. Deceptively representing to Plaintiffs Jill and John Schreidl and Colorado Class Members that it did not use Pixel when it did.

1 468. Defendant knew or should have known that its conduct was of the nature
2 prohibited by the Colorado Consumer Protection Act.

3 469. Defendant's actions also constitute deceptive trade practices because Defendant
4 knew it failed to disclose to Plaintiffs Jill and John Schreidl and Colorado Class Members that
5 their healthcare related communications via the Web Properties would be disclosed to Facebook.

6 470. Defendant's actions also constitute deceptive trade practices because Defendant
7 intended that Plaintiffs Jill and John Schreidl and Colorado Class Members rely on its deceptive
8 and unfair acts and practices and the concealment and omission of material facts in connection
9 with Defendant's offering of goods, merchandise and services.

10 471. Specifically, Defendant was aware that Plaintiffs Jill and John Schreidl and
11 Colorado Class Members depended and relied upon it to keep their communications confidential
12 and Defendant instead disclosed that information to Facebook.

13 472. Contrary to its duties as a medical provider and its express promises of
14 confidentiality, Defendant deployed the Pixel to disclose and transmit Plaintiffs Jill and John
15 Schreidl's and Colorado Class Members' personally identifiable, non-public medical
16 information, and the contents of their communications exchanged with Defendant to third
17 parties, *i.e.*, Facebook.

18 473. Defendant's disclosures of Plaintiffs Jill and John Schreidl's and Colorado Class
19 Members' Private Information were made without their knowledge, consent, or authorization,
20 and were unprivileged.

21 474. The harm arising from a breach of provider-patient confidentiality includes
22 erosion of the essential confidential relationship between the healthcare provider and the patient.

23 475. Defendant willfully, knowingly, intentionally, and voluntarily engaged in the
24 aforementioned acts when it incorporated the Meta Pixel on its Web Properties, with knowledge
25 of the Pixel's purpose and functionality, and further utilized the benefits that Pixel provides
26 website owners to the detriment of Plaintiffs Jill and John Schreidl and the Colorado Class
27 Members.

28 476. Plaintiffs Jill and John Schreidl and the Colorado Class Members could not have

1 avoided the harms described herein through the exercise of ordinary diligence.

2 477. As a result of Defendant's actions, Plaintiffs Jill and John Schreidl and Colorado
3 Class Members have suffered harm and injury.

4 478. Defendant's unlawful conduct is ongoing. Thus, injunctive and declaratory relief
5 is necessary and appropriate to prevent further violations.

6 479. Plaintiffs Jill and John Schreidl and Colorado Class Members have been damaged
7 as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just
8 compensation, including monetary damages.

9 480. Plaintiffs Jill and John Schreidl and Colorado Class Members seek appropriate
10 relief for these injuries, including but not limited to damages that will reasonably compensate
11 Plaintiffs Jill and John Schreidl and Colorado Class Members for the harm to their privacy
12 interests as a result of Defendant's violation of the Colorado Consumer Protection Act.

13 481. Plaintiffs Jill and John Schreidl and Colorado Class Members seek all other relief
14 as the Court may deem just and proper, including all available monetary relief, injunctive and
15 declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

16
17 **WHEREFORE**, Plaintiffs Cheryl McCulley, Rebecca Blount, Cindy Freriks, Jill
18 Schreidl, John Schreidl and Demetria Ann Santiago Laboy respectfully pray for judgment in
19 their favor and against Defendant Banner Health as follows on all Counts where such relief is
20 applicable:

- 21 A. For an Order certifying the Classes (as defined herein) and
22 appointing Plaintiffs as Class Representatives and Plaintiffs'
counsel as Class Counsel;
- 23 B. For equitable relief enjoining Defendant from engaging in
24 the wrongful conduct complained of herein pertaining to the
25 misuse and/or disclosure of Plaintiffs' and Class Members'
26 Private Information, and from refusing to issue prompt,
complete and accurate disclosures to Plaintiffs and Class
Members;
- 27 C. For equitable relief compelling Defendant to utilize
28 appropriate methods and policies with respect to consumer
data collection, storage and safety, and to disclose with
specificity the type of PII and PHI disclosed to third parties;

- 1 D. For equitable relief requiring restitution and disgorgement of
2 the revenues wrongfully retained as a result of Defendant's
3 wrongful conduct;
4 E. For an award of actual damages, compensatory damages,
5 statutory damages and statutory penalties, in an amount to be
6 determined, as allowable by law;
7 F. For an award of punitive damages, as allowable by law;
8 G. For an award of attorneys' fees and costs, and any other
9 expense, including expert witness fees;
10 H. Pre- and post-judgment interest on any amounts awarded and
11 I. Such other and further relief as this Honorable Court may
12 deem just and proper.

13 **DEMAND FOR JURY TRIAL**

14 Plaintiffs hereby demand that this matter be tried to a jury on all Counts that permit trial
15 by jury.

16 Respectfully submitted,

17 **ZIMMERMAN REED LLP**

18 Dated: June 1, 2023

19 By: s/ Hart L. Robinovitch

20 Hart L. Robinovitch (AZ SBN 020910)
21 14646 North Kierland Blvd., Suite 145
22 Scottsdale, AZ 85254
23 Telephone: (480) 348-6400
24 Facsimile: (480) 348-6415
25 Email: hart.robinovitch@zimmreed.com

26 **ALMEIDA LAW GROUP LLC**

27 David S. Almeida (*pro hac vice forthcoming*)
28 Elena A. Belov (*pro hac vice forthcoming*)
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

Attorneys for Plaintiffs & the Classes

EXHIBIT A

Pages 1 - 46

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

Before The Honorable William H. Orrick, Judge

In Re Meta Pixel Healthcare)
Litigation) NO. CV 22-03580-WHO
) CV 22-05753-WHO
) CV 22-06020-WHO
) CV 22-06665-WHO
)
)
)

San Francisco, California
Wednesday, November 9, 2022

TRANSCRIPT OF PROCEEDINGS

APPEARANCES:

For Plaintiffs:

SIMMONS HANLY CONROY LLC
112 Madison Avenue, 7th Floor
New York, NY 10016
BY: JAY BARNES, ESQUIRE
ERIC JOHNSON, ESQUIRE

KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211
BY: NICOLE RAMIREZ, ESQUIRE

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, WA 98103
BY: BETH E. TERRELL, ESQUIRE

For Defendants:

GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166
BY: LAUREN R. GOLDMAN, ESQUIRE

Reported By: Pamela A. Batalo, CSR No. 3593, RMR, FCRR
Official Reporter

BY: MICHAEL RHODES, ESQUIRE

Wednesday - November 9, 2022

2:30 p.m.

P R O C E E D I N G S

---000---

THE CLERK: Calling Civil Matter CV 22-3580 and all consolidated and related matters in Doe vs. Meta Platforms, Inc.

Counsel, if you would please come forward and state your appearance.

Any counsel who are going to be addressing the Court via the video connection, if you would use the raise-hand feature, that will help me to get you promoted.

MR. BARNES: Good afternoon, Your Honor. Jay Barnes from Simmons Hanly Conroy on behalf of the plaintiffs. I'm going to introduce my team so we are more efficient.

THE COURT: Okay.

MR. BARNES: I'm going to be arguing today on why the plaintiffs are likely to succeed on the merits of the claims.

Beth Terrell is here from Terrell Marshall. Ms. Terrell will be answering, to the extent the Court has any questions, about irreparable harm, balance of the equities, public interest, scope of the injunction, and what we know about the filter.

Nicole Ramirez is here from the Kiesel firm. She will speak to Facebook Meta -- sorry -- Meta. I've got to remember to call them Meta, not Facebook -- as to the timing of the

1 motion and Meta's simultaneous arguments that were both too
2 early and too late in bringing the motion.

3 And then Mr. Johnson is my colleague from Simmons Hanly
4 Conroy. He is with us today and has been with us helping to
5 prepare.

6 In addition, I have a sort of housekeeping question. We
7 have some slides to demonstrate some things that were in the --
8 what we've submitted. We've provided them to defense counsel.
9 We have someone ready to operate them. I wanted to make the
10 Court aware of that, make sure that was okay with Your Honor.
11 We have paper copies as well.

12 **THE COURT:** If you know how to operate it, that's
13 great. And if you want to give me paper, that's also fine.

14 **MR. BARNES:** Okay. Thank you, Your Honor.

15 **THE COURT:** It would be easier to do the paper, but --

16 **MR. BARNES:** Okay.

17 **MS. GOLDMAN:** Good afternoon, Your Honor. Lauren
18 Goldman from Gibson Dunn appearing on behalf of Meta. I'm here
19 with Michael Rhodes from Cooley, and my colleagues from Gibson
20 Dunn, Elizabeth McCloskey and Abby Barrera.

21 I will be arguing the motion.

22 **THE COURT:** Great. Good afternoon to everybody.

23 I have -- I may upend your presentations a little bit. I
24 have some preliminary thoughts and some initial questions that
25 I'd like answered before we get -- before I hear what you've

1 prepared.

2 So, first, the plaintiffs are seeking a mandatory
3 injunction so the law and the facts need to be clearly in favor
4 of their argument. The plaintiffs filed a declaration with
5 their reply from Professor Wilson. I'm not going to strike
6 that, but I will allow Meta to file a response to it. And I'd
7 like a declaration within two weeks. I don't want briefing. I
8 want a declaration that responds to what he has to say.

9 But I do have questions, and so, first, my understanding
10 is that when plaintiffs log into a patient portal on their
11 medical provider's website, Meta's pixel transmits that
12 information to Meta. The information includes their status as
13 patients and the associated URLs, as well as the prior page
14 visited by the patient.

15 And so, Ms. Goldman, my first question is, is that right?
16 And then how can a Facebook user prevent disclosure of that
17 information to Meta?

18 **MS. GOLDMAN:** Your Honor, that is not correct.

19 **THE COURT:** Okay.

20 **MS. GOLDMAN:** I believe that when -- first of all --
21 let me just take a step back.

22 That only happens if the healthcare provider has installed
23 the pixel on the patient portal page, which healthcare
24 providers are not supposed to do under Meta's terms which say
25 don't send us any information that you don't have the right to

1 send us and don't send us any health information, even if you
2 think you do have the right to send it to us.

3 The second problem with that sequence of events that the
4 plaintiffs have said is that it will vary from provider to
5 provider depending on exactly how the web provider has
6 configured the pixel. Meta gets the information that the web
7 developer chooses to send.

8 Third, the fact that somebody has clicked on a login
9 button doesn't mean that they are a patient. They may not have
10 an account at all. They may not have -- they may be logging on
11 on behalf of somebody else. I think it's very variable and
12 unclear what would be communicated to Meta under those
13 circumstances.

14 Fourth, Meta has filters to prevent the collection of even
15 potentially sensitive information, as we indicated in the
16 Wooldridge declaration. So that information may not come to
17 Meta.

18 So there are a number of reasons why I think what the
19 Court just said is not -- not accurate, most of the time.
20 Certainly is not accurate always.

21 Prior URLs, I think that will depend on the way in which
22 the pixel is configured on that website by that medical
23 provider.

24 One thing that's true -- and you can cut me off if this is
25 not directly responsive --

1 **THE COURT:** You're doing fine. I have a feeling I'm
2 going to hear something else from the plaintiffs, but go ahead.

3 **MS. GOLDMAN:** That's fine, Your Honor.

One thing that is repeatedly conflated in the plaintiffs' papers and in their expert declaration from Mr. Smith is the difference between browsing data, which we know is perfectly okay under the Ninth Circuit's *Smith* decision, and actual patient information, which is what we're here to debate today, right? So their strongest example of somebody receiving ads related to a medical condition comes from their expert, Mr. Smith himself, who said, "Well, I went on a bunch of publicly available websites, and I did some searches about ulcerative colitis, and I received ads for support groups for ulcerative colitis." Now, he was just doing ordinary browsing. That had nothing to do with logging in.

16 But I think the most direct answer to the Court's question
17 is that if somebody -- if -- it really depends on how the pixel
18 is configured by the healthcare provider.

19 Now, the Court had --

20 **THE COURT:** I had one question. So you've taken the
21 premise of my question and said it's not true, so I'm
22 interested in that, and I'll hear from the plaintiffs on that.
23 But to the extent that -- put it this way. What can a Facebook
24 user -- this is my real question -- do when the issue is not
25 the advertising; the issue is the transmission of patient

1 information under the way that the plaintiffs have described it
2 from the healthcare provider to Facebook -- to Meta? What can
3 a consumer do to stop that?

4 **MS. GOLDMAN:** Well, they can do several things,
5 Your Honor. One is that they can disconnect their "Off
6 Facebook Activity" --

7 **THE COURT:** That's advertising. I'm talking about the
8 communication from the provider to Meta. Okay?

9 **MS. GOLDMAN:** Well, most providers, it is worth
10 repeating, will not be sending this information to Meta because
11 it violates Meta's contracts for them to be doing that. The
12 Smith declaration only deals with five providers, and the one
13 that he focuses on the most is Novant Health, and it's clear
14 from the way that he describes -- this is at, I think,
15 paragraph 168 of his declaration -- Novant said, "We
16 misconfigured the pixel and therefore we may have accidentally
17 sent health information to Meta." That's on the healthcare
18 provider, not on Meta.

19 But in terms of what people can do, they can disconnect
20 their information which will dissociate their "Off Facebook
21 Activity" from their Facebook account for all but very limited
22 safety and security purposes, or they can pick up the
23 telephone. And the reason why that is relevant is not because
24 I am belittling the importance, Your Honor, of ability to use
25 medical portals in this day and age; it's because we're here on

1 a mandatory injunction, and so the plaintiffs have to show that
2 they are facing serious and extreme irreparable harm that can't
3 be remedied in money damages.

4 Mr. Doe was the only one of the four plaintiffs who
5 submitted a declaration in support of this motion, and he said
6 that he has stopped using the MedStar portal, and he looks
7 forward to using it again when MedStar gets its act together
8 and removes not just Meta's pixel but all of the other pixels
9 from its patient portal.

10 So what they can do is they can pick up the phone, and if
11 they can later show that it is Meta's fault that they were
12 inconvenienced and that Meta is legally liable to them, they
13 can sue Meta for damages.

14 **THE COURT:** Who would you like them to call?

15 **MS. GOLDMAN:** Their doctor. Their doctor. Their
16 hospital. There is -- there are many, many people out there
17 who don't have computers and don't use these portals as their
18 sole means of communication with their doctors.

19 Mr. Doe, who is the only plaintiff here who testified who
20 put in -- who put in a declaration said that he's not using the
21 portal except in a medical emergency; that he's picking up the
22 phone and calling or sending an email.

23 **THE COURT:** Okay. All right.

24 Let me hear from the plaintiffs. I don't know,
25 Mr. Barnes, if that's you.

1 **MR. BARNES:** I think this covers what I was going to
2 speak to, Your Honor. If I may, may I approach --

3 **THE COURT:** Sure.

4 **MR. BARNES:** -- and hand up our slides. And
5 Mr. Strong is working on getting the technology going.

6 I think your first question, Your Honor, if my notes are
7 correct, is you said when a patient goes to one of these
8 provider properties and clicks to log in to the portal, is
9 their status as patients and associated URLs transmitted to
10 Meta through the pixel. And our answer to that question is
11 yes.

12 If you look at the slides --

13 **THE COURT:** This did come from your expert so I'm
14 hoping that was the answer. Go ahead.

15 **MR. BARNES:** From our experts, yes. And if you look
16 at the slides we've provided you, Slide No. 2 is -- Mr. Strong
17 is going to show Slide No. 2. This will be a lot smoother now.

18 **THE COURT:** All right.

19 **MR. BARNES:** So Slide No. 2 is the home page at the
20 MedStar Health website. You can see that it's clearly targeted
21 towards patients. "MedStar Health" is in the name. At the
22 top, there is a link to the patient portal.

23 And what Mr. Smith showed -- this is depicted in paragraph
24 18 of the Smith declaration -- if the patient clicks on the
25 patient portal and they are then taken -- they are then shown

user's ID. That is the identifier for the pixel that is deployed by the website. So in this case, that's MedStar's specific pixel number that gets sent to Meta telling Meta, "Hey, this is the account for this particular property. Go put this information in whatever tranche of data you have for MedStar."

The next thing I want to focus on is "ev," and "ev" stands for "event." I would note that all of this information about what these things mean is in paragraph 27 of the Smith report. Meta did not challenge any of this in its response.

So "ev" is a subscribed button click. What does that mean? Well, it means that the person engaged in a button click as also described in the Wooldridge declaration.

The next thing I want to pop out is "dl." "Dl" shows the page where the person clicked the button. It is medstarhealth.org/mymedstarpatientportal.

The next thing I want to point out is button features.

This shows that by clicking the button, the user is going to be taken to the destination of `cernerhealth.com/oauth/` authenticate.

Cerner Health, as Your Honor is probably aware, is one of the biggest patient portal -- third-party patient portal providers in the country, medical record providers in the country.

Let's go to the next one. The next one is button text.

1 In this case, it was a click of the login button. This is
2 important for the contents. You haven't asked any questions
3 about the wiretapped contents portion of the brief, but login
4 isn't just some information concerning the substance, purport,
5 or meaning of this communication. It is the communication
6 itself. And that's a communication that has meaning,
7 particularly in the context of the destination is going to
8 Cerner Health and the page where they're at is the MyMedStar
9 patient portal.

10 If we could go to the next one.

11 The next one are the features of the page where the
12 patient is, and so this is MyMedStar/Your Patient
13 Portal/MedStar Health.

14 All of this information is bundled up in a transmission
15 that goes to Meta as soon as the patient clicks that button to
16 log in, or there is another button they saw. I think it was
17 sign up for the patient portal. When you sign up, the same
18 thing would happen.

19 It is true, it does not happen on every medical provider's
20 website in the country. We've identified at least 660 of them
21 that we sent to Meta, but it's also true that it happens on a
22 lot of medical providers' websites, and it's also true that
23 Meta is able to distinguish where this is happening.

24 So that was your first question, does it disclose this.
25 We think through our expert reports, the answer is yes.

1 Ms. Goldman raised a defense we've heard in every one of
2 these hospital cases that we've brought around the country, is
3 that, well, there may be false positives. And that is true, in
4 some circumstances, there may be false positives. But the
5 existence of a false positive does not undue Meta's promise to
6 its users or the violation of rights for those patients who are
7 positive positives.

8 And the way I like to talk about this in cases is if Meta
9 got a list -- asked Sutter Health in Northern California, "Send
10 us a list of all of your patients, and if you want to, you can
11 put -- two percent of those can be fake names, and then that
12 way we won't know -- we won't know for sure. Some of them are
13 false positives." Would that negate the privacy violation to
14 the 98 percent who were positive positives? We think not.

15 And the people who are accessing these patient portals and
16 successfully signing in and signing out, in the vast majority
17 of cases, the only way you get that patient portal account is
18 if you're a patient or you're a proxy for a patient. It's not
19 in our briefs, but proxies for patients are protected by HIPAA
20 as well in the HIPAA De-Identification Rule.

21 That was your first question. If I have not answered it
22 completely, I would be happy to elaborate further.

23 **THE COURT:** So Ms. Goldman raised a number of
24 distinctions between what I had said my understanding was and
25 what she says reality is. Among the things that she indicated

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5

5

6

7
8
9
0

1

2
3
4

5
6
7
8
9
0
1
2
3
4
5

1

2

1

3

4

5

1 so long as there is not informed written consent under HIPAA.
2 Meta argues you can't apply that if you are not a medical
3 provider. We don't believe that's true. There is a federal
4 statute. I believe it's 42 U.S.C. 1320d-6. I think we cited
5 it in our papers. If my memory is incorrect --

6 **THE COURT:** You cited a number of laws relating to
7 this.

8 **MR. BARNES:** Okay. So that's how we would respond to
9 this argument that this isn't -- Meta saying "this isn't our
0 problem." Meta has an obligation, a contractual obligation and
1 they have a broader obligation to make certain that they are
2 not receiving this data; that we think their response is
3 essentially an admission that there is some data at issue in
4 this case that they should not be receiving, like the patient
5 portal login information.

6 **THE COURT:** Well, so that sort of brings me to the end
7 of the analysis, which is how to deal with -- if you were going
8 to get injunctive relief, when you describe that there is some
9 information that -- that Meta may be -- is receiving and you
10 have one plaintiff who has -- who you've identified in these
11 papers and you're seeking a mandatory injunction to cover 660
12 providers, how do you get there? And may I say, I've read all
13 your papers, so --

4 **MR. BARNES:** Your Honor, that's a very fair question.
5 That's a question we talked about a lot in preparing.

- 1
- 2
- 3
- 4
- 5
- 6
- 7

8
9
0
1
2
3
4

5
6
7

8
9
0
1
2
3

4

5

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5

4

5

6
7
8

9.0

1
2

3
4
5
6
7
8
9

0
1
2

3
4

5

1

2

3

6

10

11

19

20

21

22

23

24

25

1 developers, and we say two things. We say don't send us
2 anything that you don't have the legal right to send us and
3 don't send us health information or financial information, even
4 if you think you have the right. Even if you think your
5 disclosures are terrific and you have total consent, don't send
6 us that stuff. We don't want it.

7 And then we have an over-inclusive filter system -- some
8 of this is provisionally under seal so I'm going to be careful
9 in the way that I talk about it -- but we have an
10 over-inclusive system that classifies our partners, these web
11 developers, not as HIPAA-covered, okay, because we go beyond
12 that. We say if it has anything to do with health, then we
13 operate our systems, which are described in the Wooldridge
14 declaration in the portion that are sealed, and we have
15 multiple different backstopping ways of preventing this
16 information from coming into Meta. So we're doing the best we
17 can to prevent that information from coming in and being used.
18 Okay?

19 And the reason why we set it up that way is that Meta's
20 engineers have determined that prevention and detection are the
21 best ways to prevent the receipt of potentially sensitive
22 information at scale. Now, the Court is certainly aware that
23 enormous quantities of information come into Meta every day, so
24 for Meta to sit there and say did this person violate HIPAA and
25 did this bank violate the banking regulations and did the video

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5

5
6
7
8
9
0
1
2
3
4
5
6
7
8
9
0
1
2
3
4
5

0
1
2
3
4
5

- 1
- 2
- 3
- 4
- 5

6
7
8
9
0
1
2
3
4
5

26
27
28
29
30
31
32
33
34
35

1 Instagram -- it's not the right analogy here.

2 Meta scientists, who are charged with making sure that
3 Meta is not receiving sensitive information which Meta doesn't
4 want, have determined that the best way to prevent that is with
5 this detection and prevention system that we've described and
6 that we are happy to describe in greater detail in a response
7 to the Wilson declaration.

8 But I don't want to suggest that we're saying this is the
9 web developer's problem. Meta very much thinks it is Meta's
10 problem, which is why it fulfills its promise to users to
11 contractually require its partners to avoid sending it
12 Meta-sensitive information and information that they don't have
13 the legal right to send and why Meta takes these steps to
14 filter out information that may come in, despite those
15 contractual obligations. So it's just not correct to say that
16 we are not fulfilling our promise.

17 In addition, Mr. Barnes said, Well, 'require' means block.
18 That's exactly what the filter -- the filtration system is
19 intended to do. Meta's disclosures, with respect, Your Honor,
20 are very clear. They say, We're going to get information about
21 the things you do on other websites, and we're going to require
22 our partners to have the legal rights to send those -- that
23 information to us. That's exactly what Meta is doing, both
24 contractually and technologically. So the fact that some level
25 of information -- and plaintiffs haven't tried to quantify

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8

9
0

- 1.
- 2.
- 3.
- 4.
- 5.

6

7

8
9

0

1
2
3
4
5

1 || decision in Zynga.

2 **THE COURT:** But if it includes the URL information,
3 isn't that more? If it establishes through a patient portal
4 that somebody is a patient, do you think that's just the
5 contact information, contact --

6 MS. GOLDMAN: Well, the Wiretap Act and CIPA,
7 Your Honor, don't protect all information. They protect the
8 content of a communication. "Content" is defined under the
9 Wiretap Act as "the substance, purport or meaning of a
0 communication," so it's specific. It's a conversation between
1 two people. That's what the court said in *Zynga*.

2 So there's two kinds of URLs -- there are many kinds of
3 URLs, but there are two that are sort of relevant here. One is
4 just record information about where something is going on the
5 Internet, and that's not content. Detailed URLs might be
6 content, depending on what they are and what the search terms
7 reveal.

8 But I'd point the Court to a decision from another judge
9 of this district in the *Hammerling vs. Google* case because in
10 that case, Google was receiving lots of information about how
11 people used apps, and some of those apps tracked things like
12 menstruation and pregnancy --

3 **THE COURT:** But Google wasn't doing anything with it.
4 Isn't that a distinction between this and *Hammerling*?

5 MS. GOLDMAN: No. Google was analyzing that

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8

9
0

1

2
3
4

5
6
7
8
9

0
1
2
3
4
5

1 This is just a very specific statute, and the fact that
2 this is debatable and the fact that, frankly, even more
3 broadly, it's debatable whether *Smith* applies here -- we don't
4 think it is debatable. We think *Smith* forecloses this
5 litigation. The Court seems like it has a lot of questions
6 about that --

7 **THE COURT:** I don't actually think that that's the
8 case.

9 **MS. GOLDMAN:** Okay. But we would submit that it is at
10 least debatable, and if it is debatable, then they can't get a
11 preliminary mandatory injunction.

12 But going back to the Judge Chhabria case, first of all,
13 that one is clearly debatable whether -- whether it's even
14 correct because, as we said in our brief, Judge Chhabria -- and
15 I'm going to get into this -- was construing a different
16 contractual term in a totally different context, and we can
17 talk about that, but a court in Illinois came out the exact
18 other way. So clearly it's debatable. It's not something
19 where they can get preliminary injunctive relief.

20 But the language at issue in that case was if an
21 application asks permission from someone else to access your
22 information, the application will be allowed to use that
23 information only in connection with the person who gave the
24 permission. And so the key word was "allowed." Here it's
25 "required." And Judge Chhabria rejected Facebook's argument

1 that the only possible interpretation of that language was that
2 it meant we just tell app developers what to do and that's it.
3 Okay? He said "allowed" could mean a technological block. It
4 could mean that you do some level of actively policing. It's
5 ambiguous.

6 Well, if it's ambiguous here, we win because -- we win
7 this motion, and we'll discuss all of this, I'm sure, in
8 greater detail on the motion to dismiss because they can't get
9 a mandatory injunction unless they prove basically that they're
10 right because under *Marlyn Nutraceuticals*, a preliminary
11 injunction is not granted when anything is even remotely
12 doubtful about the merits of the plaintiff's case.

13 There were also different facts there because the
14 plaintiffs there alleged that Facebook did nothing to enforce
15 its purported policy against tens of thousands of app
16 developers who were freely making off with sensitive user
17 information, and here we have introduced a declaration and we
18 will introduce more evidence about this, that Facebook is
19 actually making very extensive efforts, the best that it can,
20 and plaintiffs really have not suggested anything better, which
21 is a problem with their bid for an injunction, to enforce this
22 promise and to make sure that they -- that Meta is not
23 receiving sensitive information.

24 Third, again, it's a different legal standard because this
25 is a preliminary injunction and not the motion to dismiss. We

1 don't have the burden. They do. It's a different context.
2 *Cambridge Analytica* was about what third parties could do with
3 information that they were obtaining from the Facebook
4 platform. This is different. This is about what Meta does
5 with information that web developers unilaterally control and
6 decide to send to Meta.

7 So when you're construing the word "require," you have to
8 construe it against that background: What would a reasonable
9 person think Meta is able to do in terms of requiring. We
10 require it contractually, and we block it -- we try our best to
11 block it when they break that contract and send it to us. That
12 is a very reasonable interpretation of "require." And as I
13 mentioned, there is different decisions coming out different
14 ways.

15 And this is really a broader point because all of the --
16 all of the cases on that slide that Mr. Barnes, I believe,
17 showed you, the *Google Cookie* case, *In Re Facebook Internet*
18 *Tracking*, they're all about disclosures that the courts found
19 to be affirmatively misleading in the context.

20 So *Facebook Internet Tracking*, which they spent a lot of
21 time on in their brief and I'm sure the Court has read --
22 that's the Ninth Circuit case -- Facebook said, We receive your
23 user ID when you are logged in, and the Court said, Well, that
24 could mean to a reasonable person that we don't receive your
25 user ID when you're logged out of Facebook. And for an

1 eleven-month period, over ten years ago, Facebook was receiving
2 that logged-out data as a result of a technical glitch, I will
3 say as an aside because we handled that case. But -- okay. If
4 I say we received this when you're logged in, you could infer
5 that I don't receive it when you're logged out.

6 One of the Google cases that they cited, the *Google Cookie*
7 case, the one from district court here, said it was the same
8 thing. The language said -- of the policy said -- oh, it
9 was -- it was Judge Koh's decision in the case about Google
10 Sync. Google's disclosure said you don't have to share any
11 personal information with us in order to use Google Chrome, and
12 it turned out that even when people weren't synced up and they
13 weren't sharing personal information, Google Chrome was still
14 collecting information about us -- about them. And Judge Koh
15 said a reasonable user could have concluded, based on Google's
16 disclosures, that if he or she used Chrome without Sync, his or
17 her personal information would not be sent to Google.

18 There is nothing comparable here, Your Honor. Our
19 disclosures were broad and unambiguous. When you travel around
20 the Internet and you interact with third-party apps, they can
21 send us information about what you do on those apps regardless
22 of whether you are logged in or logged out of Facebook. Broad,
23 clear, definitive. That's what we do.

24 And we explained that that's how Facebook is free. It's
25 because we gather this data and we use it for ads. And here

- 1
- 2
- 3
- 4
- 5
- 6

7
8

9
0

1

2

3
4
5

6

1
2
3
4
5
6
7
8
9
10
11

2
3

4

5

1 motion regarding the contract interpretation. We disagree.
2 This is a consumer contract of adhesion. If it's ambiguous,
3 the consumer wins. That is black letter law. I don't know
4 that we have a case that we cited in our brief, but I don't
5 think that's a controversial statement.

6 The second is Ms. Goldman was talking about contents. She
7 said what is depicted in Slide No. 3, which is the -- literally
8 it says login is not content, and she said that's not a
9 communication. Well, the ECPA also defines what an electronic
10 communication is. I guess -- let me back up a step.

11 When she described the definition of "contents," she left
12 out some important words. "Contents" is not the substance,
13 purport, or meaning of the communication. "Contents," under
14 the Wiretap Act, is any information concerning the substance,
15 purport, or meaning of the communication. So a description of
16 the communication is contents. Something that leads you to
17 connect the dots of what the underlying communication means is
18 contents because it is some information about the substance,
19 purport, or meaning.

20 But she also said it's not an electronic communication.
21 18 U.S.C. 2510, sub 12, defines "electronic communication" in
22 about as broad a way as one could possibly do so. It means,
23 "Any transfer of signs, signals, writing, images, sounds, data,
24 or intelligence of any nature transmitted in whole or in part
25 by," and then there is a long list that essentially are

1

2
3
4
5
6
7
8
9
0

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3

4
5

1 it over to Ms. Terrell.

2 **THE COURT:** Let me ask you one question on the
3 Federal -- we have been talking about the Wiretap Act. Given
4 one-party consent, the question is whether the exception -- an
5 exception applies, and, one, the fundamental issue, I think, is
6 whether advertising as a business purpose would also be
7 tortious and -- or criminal. And so I guess the question I
8 have is what's your perspective on that topic and how narrowly
9 or broadly should I look at Meta's purpose at this stage -- at
10 this stage, particularly when you're seeking an injunction, a
11 mandatory injunction.

12 **MR. BARNES:** I think you should look -- I think you
13 should look narrowly. I didn't think about it in the terms of
14 narrowly or broadly. Advertising in and of itself, just
15 broadly speaking, is not tortious activity, but there are
16 certainly circumstances in which taking someone's information
17 without their authorization is tortious activity, and then when
18 you use that information you have obtained without
19 authorization for advertising, that could be tortious activity
20 as well.

21 So I guess one analogy that I'm thinking on the fly here
22 is if one business stole another business's trade secrets
23 through a wiretap act that one party consented to and then they
24 used that for a business purpose, having stolen it, would that
25 wiretap have violated -- fall to the exception to the

1 exception? I think so if it did so for the purpose of
2 basically stealing information it was not authorized to
3 receive.

4 **THE COURT:** If you could prove it. If there was
5 intent. I mean, that's the --

6 **MR. BARNES:** And let me back up because there is two
7 other things. I think these are mentioned in our brief, but
8 the -- it's a violation of the Constitution or laws -- criminal
9 or tortious violation of the Constitution or laws of the
10 United States or any state is what the exception to the
11 exception says. And we think we fit under that for at least
12 two reasons. One -- three reasons. One is the analogy I just
13 came up with here. The second is the HIPAA 42 U.S.C. 1320d-6.
14 And the third is if you look on Slide 5, I think, where we say
15 law and facts clearly favor plaintiffs' position, we list these
16 six hospital cases.

17 It's not just whether Facebook has the intent, it's
18 whether the party that purportedly consented had a tortious
19 intent. And so far we've had decisions on motions to dismiss
20 in six cases and so far we have prevailed in all six cases.
21 Now, not on every claim in every case, right, but we've
22 prevailed. In every single case, the court has either found
23 it's a violation of state criminal statute, common law,
24 statutory tort, breach of contract. And we think that's highly
25 relevant here to whether the exception to the exception

1 applies.

2 **THE COURT:** Okay. All right. Thank you.

3 **MR. BARNES:** And -- Ms. Terrell. Thank you.

4 **MS. TERRELL:** Good afternoon, Your Honor.

5 There are three issues I want to address. One is the
6 scope of the injunction generally, and I want to focus
7 specifically on the second part of the injunction that we asked
8 for, which is Meta's use of the historical data it's already
9 gathered.

10 The second issue I want to talk about is why the filter it
11 has described in the Wooldridge declaration is not an adequate
12 alternative to an injunction.

13 And the third is to offer my unsolicited thoughts on what
14 the Wooldridge declaration should actually include if we are
15 actually going to have the kind of evidence and facts before
16 the Court that I think should be there.

17 So the first issue is the injunction that we seek, the
18 second part of it is focused on enjoining Meta from
19 disseminating and/or using patient information and
20 communications that it has intercepted from HIPAA-covered
21 entities through its use of the Meta pixel, and why I think
22 that's so important is Meta still has a cache of health
23 information in its systems, so far as we know. It doesn't deny
24 that. It hasn't indicated that as a result of adopting this
25 filter or these other tools to address some of these problems

- 1
- 2
- 3
- 4
- 5
- 6

7
8
9
0

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0

1
2
3
4
5

1
2
3
4
5
6
7
8
9
0
1

2
3
4
5
6

17
18
19
20
21
22
23

4

5

1 just medical apps or is it also websites or the efficacy of it.
2 There is nothing in there about the metrics of the amount of
3 data that it is being sent, that Meta is receiving, the amount
4 that it's blocked, nothing. Yet Meta and Facebook were being
5 grilled for a number of years by DFS about exactly those
6 issues.

7 In addition, the filter has limited utility. It does not
8 block Meta from receiving the data. It only prevents -- and
9 this is from the Wooldridge declaration -- quote, the detected
10 data from being ingested into Meta's ad ranking and
11 optimization systems. That's the Wooldridge declaration at
12 paragraph 8.

13 Meta does not provide any evidence that its filter
14 actually stops it from receiving the data. The data is not
15 blocked. It is just not directed to those two systems so it is
16 arguably not used for ads. And it's the knowing receipt of
17 that information that is what triggers the laws that we're
18 talking about here.

19 In addition, the filter does not identify obviously
20 health-related terms like "health," "patient," and "provider
21 name" like MedStar. How do we know that? We know that from
22 Slide 4, and that's the -- one of the slides that Mr. Barnes
23 already walked through because Slide 4 -- well, that was
24 reported in August of 2022. So it was well after the filter
25 was in place, well after the investigation was done, and after

1 In addition, the filter -- so the filter does not address
2 the past acquisition. And so let's talk about what the
3 Wooldridge declaration does not address. I think there is five
4 important issues that are missing.

5 Number one, the genesis of the filter, why it became --
6 even came into being; the efficacy of the filter at any time,
7 including now; which systems the health data is actually
8 ingested into. It only says which ones it is not. And what,
9 if anything, Meta has done to stop using the data it already
10 gathered.

11 The final thing that's really missing from Wooldridge is
12 what, if anything, has Meta done to enforce its requirement
13 that developers only send data for which they have consent.
14 There is no evidence in the record as to what policing activity
15 Meta does at all with regard to this health information.

16 And one of the reasons why we offered the declaration of
17 Christo Wilson is that he lays out some pretty common-sense
18 ways in which Meta should interact with its developers to the
19 extent that it's finding that they are consistently repeat
20 violators of the policy.

21 But let's look at what Meta can do to prevent itself from
22 getting the data. I think it can do it on both sides. Number
23 one, it can disable the pixel on the website portals where it
24 knows that they are HIPAA-related entities. It can do that.
25 It has the technology.

1 Number two, it can tweak its filter so that the filter
2 actually prevents information that includes the login, the
3 portal-type login information that it's currently receiving.
4 That's at the issue -- at the issue in this litigation. And we
5 think it wouldn't even be that hard because as Mr. Barnes
6 noted, there are really two major providers of the patient
7 portals, and their names tend to be within the URL data that is
8 transmitted to Meta. And so if you put -- you block "Cerner"
9 and you block "Epic," along with "login" and "portal" and
10 "patient" and "health," maybe the filter would actually be
11 effective.

12 **THE COURT:** All right.

13 **MS. TERRELL:** I think that's probably the bottom line,
14 and I think that's what Mr. Wooldridge really needs to address
15 here.

16 So the injunction is not overbroad. It's actually
17 specifically tailored to what Meta could do and actually what
18 it should have already done given that it's been well aware of
19 these issues since at least 2019.

20 **THE COURT:** All right. Thank you.

21 Ms. Goldman, I will give you the last word.

22 **MS. GOLDMAN:** I will keep it very brief --

23 **THE COURT:** Yes.

24 **MS. GOLDMAN:** -- as you were very patient with me
25 earlier.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5

5
6
7
8

9
0
1
2

3
4
5
6
7
8
9
0
1
2

3
4
5

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5

7
8
9

0
1
2
3
4

5
6
7

8

9

1

2

3

4

5

CERTIFICATE OF REPORTER

I certify that the foregoing is a correct transcript
from the record of proceedings in the above-entitled matter.

DATE: Monday, November 14, 2022

Pamela Batalo Hebel

Pamela Batalo Hebel, CSR No. 3593, RMR, FCRR
U.S. Court Reporter