

MAR 14 2024

BY   
DEPUTY CLERK

1 Andrew Gunem (354042)  
TURKE & STRAUSS, LLP  
2 613 Williamson Street, Suite 201  
Madison, Wisconsin 53703  
3 (608) 237-1775  
andrewg@turkestrauss.com

Lynn A. Toops\*  
Mary Kate Dugan\*  
COHEN & MALAD, LLP  
One Indiana Square, Suite 1400  
Indianapolis, Indiana 46204  
(317) 636-6481  
ltoops@cohenandmalad.com  
mdugan@cohenandmalad.com

C. Crosby

5 Natalie A. Lyons (293026)  
6 Vess A. Miller (278020)  
COHEN & MALAD, LLP  
7 One Indiana Square, Suite 1400  
Indianapolis, Indiana 46204  
8 (317) 636-6481  
nlyons@cohenandmalad.com  
9 vmiller@cohenandmalad.com

J. Gerard Stranch, IV\*  
Andrew E. Mize\*  
STRANCH, JENNINGS & GARVEY, PLLC  
223 Rosa L. Parks Avenue, Suite 200  
Nashville, Tennessee 37203  
(615) 254-8801  
gstranch@stranchlaw.com  
amize@stranchlaw.com

10 *Counsel for Plaintiff and the Proposed Class*

\*To move for *pro hac vice* admission

11 SUPERIOR COURT FOR THE STATE OF CALIFORNIA  
12 FOR THE COUNTY OF LASSEN

2024 CV 0 07 6 5 6 4

13 JOHN DOE, individually and on behalf of  
all others similarly situated,

Case No. \_\_\_\_\_

14 Plaintiff,

CLASS ACTION COMPLAINT  
FOR DAMAGES AND INJUNCTIVE  
RELIEF BASED UPON:

15 v.

16 BANNER HEALTH

17 Defendant.

- (1) Negligence;
- (2) Breach of Implied Contract;
- (3) Unjust Enrichment;
- (4) Breach of Fiduciary Duty;
- (5) Invasion of Privacy;
- (6) Invasion of Privacy under the California Constitution, Cal. Const. Art. I § 1;
- (7) Violation of the California Invasion of Privacy Act, Cal. Penal Code § 630, *et seq.*
- (8) Violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56.06, 56.10, 56.101;
- (9) Violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; and,
- (10) Violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*

JURY TRIAL DEMANDED

FILE  
BY FAX

1 **CLASS ACTION COMPLAINT**

2 Plaintiff, JOHN DOE, Individually, and on behalf of all others similarly situated  
3 (hereinafter, "Plaintiff"), brings this Class Action Complaint against Defendant, BANNER  
4 HEALTH (hereinafter, "Banner" or "Defendant"), and alleges, upon personal knowledge as to his  
5 own actions, and upon information and belief as to all other matters, as follows.

6 **INTRODUCTION**

7 1. Plaintiff brings this class action to address Defendant's improper practice of  
8 disclosing the confidential Personally Identifying Information ("PII")<sup>1</sup> and/or Protected Health  
9 Information ("PHI")<sup>2</sup> (collectively referred to as "Private Information") of Plaintiff and the  
10 proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook"  
11 or "Meta"),<sup>3</sup> Google, LLC ("Google"), Microsoft, AppDynamics, Taboola, Pinterest, StackAdapt,  
12

13  
14 <sup>1</sup> The Federal Trade Commission defines "identifying information" as "any name or number that  
15 may be used, alone or in conjunction with any other information, to identify a specific person,"  
16 including, among other things, "[n]ame, Social Security number, date of birth, official State or  
17 government issued driver's license or identification number, alien registration number,  
18 government passport number, employer or taxpayer identification number." 17 C.F.R. §  
19 248.201(b)(8).

20 <sup>2</sup> Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and  
21 its implementing regulations ("HIPAA"), "protected health information" is defined as  
22 individually identifiable information relating to the past, present, or future health status of an  
23 individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in  
relation to the provision of healthcare, payment for healthcare services, or use in healthcare  
operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information  
such as diagnoses, treatment information, medical test results, and prescription information are  
considered protected health information under HIPAA, as are national identification numbers and  
demographic information such as birth dates, gender, ethnicity, and contact and emergency  
contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS.,  
<https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last accessed  
Apr. 16, 2020). Banner is clearly a "covered entity" and some of the data compromised in the  
Disclosure that this action arises out of is "protected health information," subject to HIPAA.

<sup>3</sup> Facebook changed its name from Facebook, Inc. to Meta Platforms, Inc. in October 2021.  
Plaintiff's reference to both "Facebook" and "Meta" throughout this complaint refer to the same  
company.

1 LinkedIn, Skai, Medallia, and potentially others via tracking technologies used on its website (“the  
2 Disclosure”).

3         2.       The Office for Civil Rights (“OCR”) at the U.S. Department of Health and Human  
4 Services (“HHS”) and the Federal Trade Commission (“FTC”) warn about the “serious privacy  
5 and security risks related to the use of online tracking technologies” present on websites or online  
6 platforms, such as Defendant’s, that “impermissibly disclos[e] consumers’ sensitive personal  
7 health information to third parties.”<sup>4</sup> OCR and FTC agree that such tracking technologies, like  
8 those present on Defendant’s website, “can track a user’s online activities” and “gather identifiable  
9 information about users as they interact with a website or mobile app, often in ways which are not  
10 avoidable by and largely unknown to users.”<sup>5</sup> OCR and FTC warn that “[i]mpermissible  
11 disclosures of an individual’s personal health information to third parties may result in a wide  
12 range of harms to an individual or others. Such disclosures can reveal sensitive information  
13 including health conditions, diagnoses, medications, medical treatments, frequency of visits to  
14 health care professionals, where an individual seeks medical treatment, and more. In addition,  
15 impermissible disclosures of personal health information may result in identity theft, financial loss,  
16 discrimination, stigma, mental anguish, or other serious negative consequences to the reputation,  
17 health, or physical safety of the individual or to others.”<sup>6</sup>

18         3.       Information about a person’s physical and mental health is among the most  
19 confidential and sensitive information in our society, and the mishandling of medical information  
20 can have serious consequences, including discrimination in the workplace or denial of insurance  
21

---

22 <sup>4</sup> Re: Use of Online Tracking Technologies, U.S. Dep’t of Health & Human Services (July 20,  
23 2023), available at [https://www.ftc.gov/system/files/ftc\\_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), attached as Exhibit A.

<sup>5</sup> *Id.*

<sup>6</sup> Re: Use of Online Tracking Technologies, Exhibit A.

1 coverage. If people do not trust that their medical information will be kept private, they may be  
2 less likely to seek medical treatment, which can lead to more serious health problems down the  
3 road. In addition, protecting medical information and making sure it is kept confidential and not  
4 disclosed to anyone other than the person's medical provider is necessary to maintain public trust  
5 in the healthcare system as a whole.

6 4. Recognizing these facts, and in order to implement requirements of the Health  
7 Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS has established "Standards  
8 for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule")  
9 governing how health care providers must safeguard and protect Private Information. Under the  
10 HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable  
11 protected health information to a third party without express written authorization.

12 5. Headquartered in Phoenix, Arizona, Banner is a massive, national health care  
13 system treating patients in six (6) western states under a mission of "*making health care easier,*  
14 *so life can be better.*"<sup>7</sup>

15 6. Despite its unique position as a massive and trusted healthcare provider, Banner  
16 knowingly configured and implemented into its website, <https://www.bannerhealth.com/> (the  
17 "Website") code-based tracking devices known as "pixels" (also referred to as "trackers" or  
18 "tracking technologies"), which collected and transmitted patients' Private Information to  
19 Facebook and other third parties, without patients' knowledge or authorization.

20 7. Defendant encourages patients to use its Website, along with its various web-based  
21 tools and services (collectively, the "Online Platforms"), to learn about Banner on its main  
22  
23

---

<sup>7</sup> <https://www.bannerhealth.com/about> (last accessed March 8, 2024) (emphasis in original)

1 homepage,<sup>8</sup> to search for health information,<sup>9</sup> to find a doctor,<sup>10</sup> to find locations,<sup>11</sup> to learn about  
2 medical conditions and treatment services,<sup>12</sup> to learn about classes and events,<sup>13</sup> to access a patient  
3 portal,<sup>14</sup> to pay bills,<sup>15</sup> and more.

4 8. When Plaintiff and Class Members used Defendant's Website and Online  
5 Platforms, they thought they were communicating exclusively with their trusted healthcare  
6 provider. Unbeknownst to them, Defendant embedded pixels from Facebook, Google, and likely  
7 others, into its Website and Online Platforms, surreptitiously forcing Plaintiff and Class Members  
8 to transmit intimate details about their medical treatment to third parties without their consent.

9 9. A pixel (also referred to as a "tracker" or "tracking technology") is a snippet of  
10 code embedded into a website that tracks information about its visitors and their website  
11 interactions.<sup>16</sup> When a person visits a website with an embedded pixel, the pixel tracks "events"  
12 (i.e., user interactions with the site), such as pages viewed, buttons clicked, and information  
13 submitted.<sup>17</sup> Then, the pixel transmits the event information back to the website server and to third  
14 parties, where it can be combined with other data and used for marketing.<sup>18</sup>

15  
16  

---

<sup>8</sup> <https://www.bannerhealth.com/> (last acc. Mar. 8, 2024).

17 <sup>9</sup> E.g., search for "chest pain," avail. at  
<https://www.bannerhealth.com/search?query=chest%20pain> (last acc. Mar. 8, 2024).

18 <sup>10</sup> <https://www.bannerhealth.com/physician-directory> (last acc. Mar. 8, 2024).

19 <sup>11</sup> <https://www.bannerhealth.com/find-a-location> (last acc. Mar. 8, 2024).

20 <sup>12</sup> <https://www.bannerhealth.com/services> (last acc. Mar. 8, 2024).

21 <sup>13</sup> <https://www.bannerhealth.com/calendar> (last acc. Mar. 8, 2024).

22 <sup>14</sup> [https://account.bannerhealth.com/sign-in?\\_ga=2.66854765.237380448.1709911311-131706459.1709911311](https://account.bannerhealth.com/sign-in?_ga=2.66854765.237380448.1709911311-131706459.1709911311) (last acc. Mar. 8, 2024).

23 <sup>15</sup> <https://bannerhealth.simpleepay.com/app/login> (last acc. Mar. 8, 2024).

<sup>16</sup> See Meta Pixel, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/>  
(last accessed Mar. 19, 2023).

<sup>17</sup> See Conversion Tracking, META FOR DEVELOPERS,  
<https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking> (last  
visited May 22, 2023).

<sup>18</sup> *Id.*

1           10.     Among the trackers Defendant embedded into its Website is the Facebook Pixel  
2 (also referred to as the “Meta Pixel” or “Pixel”). By default, the Meta Pixel tracks information  
3 about a visitor’s device, including their IP address, and the pages viewed.<sup>19</sup> When configured to  
4 do so, the Meta Pixel can track much more, including a visitor’s search terms, button clicks, and  
5 form submissions.<sup>20</sup> Additionally, the Meta Pixel can link a visitor’s website interactions with an  
6 individual’s unique and persistent Facebook ID (“FID”), allowing a user’s health information to  
7 be linked with their Facebook profile.<sup>21</sup>

8           11.     Operating as designed and as implemented by Defendant, the Meta Pixel allowed  
9 Defendant to unlawfully disclose Plaintiff and Class Members’ Private Health Information  
10 alongside identifying details to Facebook. By installing the Meta Pixel on its Website, Defendant  
11 effectively planted a bug on Plaintiff’s and Class Members’ web browsers and compelled them to  
12 disclose Private Information and confidential communications to Facebook without their  
13 authorization or knowledge.

14           12.     Facebook encourages and recommends use of its Conversions Application  
15 Programming Interface (“CAPI”) alongside use of the Meta Pixel.<sup>22</sup>  
16

---

17 <sup>19</sup> See Get Started, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/get-started> (last visited May 22, 2023).

18 <sup>20</sup> See Conversion Tracking, META FOR DEVELOPERS,  
19 <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking> (last  
visited May 22, 2023).

20 <sup>21</sup> The Meta Pixel forces the website user to share the user’s FID for easy tracking via the “cookie”  
Facebook stores every time someone accesses their Facebook account from the same web browser.  
“Cookies are small files of information that a web server generates and sends to a web browser.”  
21 “Cookies help inform websites about the user, enabling the websites to personalize the user  
experience.” What are Cookies?, <https://www.cloudflare.com/learning/privacy/what-are-cookies/>  
22 (last visited Jan. 27, 2023).

23 <sup>22</sup> “CAPI works with your Meta Pixel to help improve the performance and measurement of your  
Facebook ad campaigns.” See Samir El Kamouny, How to Implement Facebook Conversions  
API (In Shopify), FETCH & FUNNEL <https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/> (last visited Jan. 25, 2023).

1           13. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to  
2 transmit information to Facebook in addition to the website owner, CAPI does not cause the user's  
3 browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website  
4 interaction, including Private Information, records and stores that information on the website  
5 owner's servers, and then transmits the data to Facebook from the website owner's servers.<sup>23, 24</sup>

6           14. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and  
7 attribution across your customer's full journey, from discovery to conversion. This helps you better  
8 understand how digital advertising impacts both online and offline results."<sup>25</sup>

9           15. Because CAPI is located on the website owner's servers and is not a bug planted  
10 onto the website user's browser, it allows website owners like Defendant to circumvent any ad  
11 blockers or other denials of consent by the website user that would prevent the Meta Pixel from  
12 sending website users' Private Information to Facebook directly.

13           16. Defendant utilized data from these trackers to market its services and bolster its  
14 profits. Meta Pixel and CAPI are routinely used to target specific customers by utilizing data to  
15 build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff's  
16 and Class Members' Private Information to create targeted advertisements based on the medical  
17 conditions and other information disclosed to Defendant.

18           17. The information that Defendant's Meta Pixel and possibly CAPI sent to Facebook  
19

---

20 <sup>23</sup> What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG,  
21 <https://revealbot.com/blog/facebook-conversions-api/> (last updated May 20, 2022).

22 <sup>24</sup> "Server events are linked to a dataset ID and are processed like events sent via the Meta  
Pixel.... This means that server events may be used in measurement, reporting, or optimization  
23 in a similar way as other connection channels." Conversions API, META FOR DEVELOPERS,  
<https://developers.facebook.com/docs/marketing-api/conversions-api> (last visited May 15, 2023).

<sup>25</sup> About Conversions API, META FOR DEVELOPERS,  
<https://www.facebook.com/business/help/2041148702652965> (last visited May 15, 2023).

1 can include the Private Information that Plaintiff and Class Members submitted to Defendant's  
2 Website, including details about the pages they browsed and the buttons they clicked, including,  
3 (i) users' keyword searches, (ii) users' physician searches, (iii) content that users viewed;  
4 (iv) activities that reveal the users' status as potential patients; and (v) identifying information.

5 18. Such information allows a third party (e.g., Facebook) to know that a specific  
6 patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class  
7 Members' Private Information to third-party marketers, who then geotarget Plaintiff's and Class  
8 Members' Facebook pages based on communications obtained via the Meta Pixel and CAPI.  
9 Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information  
10 also could reasonably infer from the data that a specific patient was being treated for a specific  
11 type of medical condition, such as cancer, pregnancy, dementia, or HIV.

12 19. In addition to the Facebook tracker and CAPI, on information and belief, Defendant  
13 installed other tracking technology which operate similarly to the Meta Pixel and transmit a  
14 website user's Private Information to other third parties.

15 20. Healthcare patients simply do not anticipate that their trusted healthcare provider  
16 will send Personal Health Information ("PHI") or other confidential medical information collected  
17 via its webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy  
18 violations in pursuit of ever-increasing advertising revenue—without the patients' consent.

19 21. Neither Plaintiff nor any Class Member signed a written authorization permitting  
20 Defendant to send their Private Information to Facebook, or any other third parties uninvolved in  
21 their treatment.

22 22. Despite willfully and intentionally incorporating tracking technology, including the  
23 Meta Pixel, potentially CAPI, and other tracking technology such as Google Analytics with Google



1 Tag Manager (“GTM”), Facebook Events, AppDynamics, Taboola, Pinterest, StackAdapt,  
2 LinkedIn, DoubleClick, Skai, Microsoft Universal Events, and Medallia, into its Website and  
3 servers, Banner has never disclosed to Plaintiff or Class Members that it shared their sensitive and  
4 confidential communications and Private Information with third parties including Facebook, and  
5 potentially others.

6 23. Defendant further made express and implied promises to protect Plaintiff’s and  
7 Class Members’ Private Information and maintain the privacy and confidentiality of  
8 communications that patients exchanged with Defendant, including in its privacy policies and  
9 elsewhere.

10 24. Defendant owed common law, statutory, and regulatory duties to keep Plaintiff’s  
11 and Class Members’ communications and Private Information safe, secure, and confidential.

12 25. Upon information and belief, Banner utilized the Meta Pixel and other tracker data  
13 to improve and to save costs on its marketing campaigns, improve its data analytics, attract new  
14 patients, and generate sales.

15 26. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff’s  
16 and Class Members’ Private Information, Defendant assumed legal and equitable duties to those  
17 individuals to protect and to safeguard that information from unauthorized disclosure.

18 27. Defendant breached its statutory and common law obligations to Plaintiff and Class  
19 Members by, *inter alia*,: (i) failing to adequately review its marketing programs and web based  
20 technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage  
21 technology that was known and designed to share web-users’ information; (iii) aiding, agreeing,  
22 and conspiring with third parties to intercept communications sent and received by Plaintiff and  
23 Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to

1 disclose their Private Information to Facebook and others; (v) failing to protect Private Information  
2 and take steps to block the transmission of Plaintiff's and Class Members' Private Information  
3 through the use of Meta Pixel and other tracking technology; (vi) failing to warn Plaintiff and Class  
4 Members; and (vii) otherwise failing to design and monitor its Website to maintain the  
5 confidentiality and integrity of patient Private Information.

6 28. Plaintiff seeks to remedy these harms and brings causes of action for  
7 (I) Negligence; (II) Breach of Implied Contract; (III) Unjust Enrichment; (IV) Breach of Fiduciary  
8 Duty; (V) Invasion of Privacy; (VI) Invasion of Privacy under the California Constitution, Cal.  
9 Const. ART. 1 § 1; (VII) Violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal  
10 Code §§ 630, *et seq.*; (VIII) Violation of the California Confidentiality of Medical Information  
11 Act ("CMIA"), Cal. Civil Code §§ 56.06, 56.10, 56.101; (IX) Violation of the Comprehensive  
12 Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; and, (X) Violation of  
13 Cal. Bus. & Prof. Code §§ 17200, *et. seq.*

14 **PARTIES**

15 29. Plaintiff, JOHN DOE, is a natural person and a resident and citizen of the State of  
16 California where he intends to remain, with a principal residence in Susanville, California in  
17 Lassen County. He is a patient of Defendant and a victim of Banner's Disclosure of his Private  
18 Information.

19 30. Defendant, BANNER HEALTH ("Banner" or "Defendant"), is a not-for-profit  
20 corporation organized and existing under the laws of the State of Arizona with its principal place  
21 of business at 2901 North Central Avenue, Suite 160, Phoenix, Arizona 85012 in Maricopa  
22 County.

23 31. Defendant's Registered Agent for Service of Process is C T Corporation System,

1 330 N Brand Boulevard, Suite 700, Glendale, California 91203.

2 **JURISDICTION & VENUE**

3 32. The Court has personal jurisdiction over Defendant because Banner transacts  
4 business in the State of California by providing medical treatment services.

5 33. This is a class action brought pursuant to Cal. Civ. Proc. Code § 382, and this Court  
6 has jurisdiction over the Plaintiff's claims because the amount in controversy exceeds this Court's  
7 jurisdictional minimum.

8 34. Venue is proper under Cal. Civ. Proc. Code § 395(a) because the injury to personal  
9 property complained of herein occurred in Lassen County.

10 **COMMON FACTUAL ALLEGATIONS**

11 **A. Background**

12 35. Founded in 1999 and based on Pheonix, Arizona, Banner is a massive healthcare  
13 system which provides treatment services to patients in Arizona, California, Colorado, Nebraska  
14 Nevada, Wyoming,<sup>26</sup> and in Alaska, through "28 hospitals and a growing network of health centers  
15 and clinics."<sup>27</sup>

16 36. On its Website, Defendant represents to patients and prospective patients that:

17 At all stages in life, you can rest assured that Banner will meet your health and  
18 medical needs through compassionate professionals and outstanding service.  
19 Headquartered in Phoenix, Arizona., Banner Health is one of the largest, nonprofit  
20 health care systems in the country and the leading nonprofit provider of hospital  
21 services in all the communities we serve.<sup>28</sup>

22 37. Indeed, Banner owns and operates numerous hospital and medical centers,  
23 including: Banner Boswell Medical Center in Sun City, Arizona; Banner Del E Webb Medical

---

23 <sup>26</sup> See generally, <https://www.bannerhealth.com/find-a-location> (last acc. Mar. 8, 2024).

<sup>27</sup> <https://www.bannerhealth.com/about/glance/history> (last acc. Mar. 8, 2024).

<sup>28</sup> <https://www.bannerhealth.com/about> (last acc. Mar. 8, 2024).

1 Center, in Sun City West Arizona; Banner MD Anderson Cancer Center at Banner Gateway  
2 Medical Center, in Gilbert, Arizona; Banner Gateway Medical Center in Gilbert, Arizona; Banner  
3 Rehabilitation Hospital West in Peoria, Arizona; Banner Ocotillo Medical Center in Chandler,  
4 Arizona; Banner Behavioral Health Hospital in Scottsdale, Arizona; Banner - University Medical  
5 Center South in Tucson, Arizona; Banner - University Medical Center Tucson in Tucson, Arizona;  
6 Diamond Children's Medical Center in Tucson, Arizona; Banner Thunderbird Medical Center and  
7 Banner Children's at Thunderbird in Glendale, Arizona; Banner Payson Medical Center in Payson,  
8 Arizona; Banner Children's at Desert in Mesa, Arizona; Banner Desert Medical Center in Mesa,  
9 Arizona; Banner Heart Hospital in Mesa, Arizona; Banner Rehabilitation Hospital East and Banner  
10 Baywood Medical Center in Mesa, Arizona; Banner Ironwood Medical Center in Queen Creek,  
11 Arizona; Banner Goldfield Medical Center in Apache Junction, Arizona; Banner Rehabilitation  
12 Hospital Phoenix, Banner Estrella Medical Center, and Banner - University Medical Center  
13 Phoenix in Phoenix, Arizona; Page Hospital in Page, Arizona; Banner Lassen Medical Center in  
14 Susanville, California; Banner Casa Grande Medical Center in Casa Grande, Arizona; Sterling  
15 Regional MedCenter in Sterling, Colorado; Banner Fort Collins Medical Center in Fort Collins,  
16 Colorado; Banner North Colorado Medical Center in Greeley, Colorado; East Morgan County  
17 Hospital in Brush, Colorado; Banner McKee Medical Center in Loveland, Colorado; Banner  
18 Churchill Community Hospital in Fallon, Nevada; Community Hospital in Torrington, Wyoming;  
19 Banner Wyoming Medical Center in Casper, Wyoming; Platte County Memorial Hospital in  
20 Wheatland, Wyoming; Washakie Medical Center in Worland, Wyoming; Ogallala Community  
21 Hospital in Ogallala, Nebraska.<sup>29</sup>

22  
23  

---

<sup>29</sup> See, "Locations," avail. at <https://www.bannerhealth.com/locations?loctype=Hospital&PageNo=1> (last acc. Mar. 8, 2024).

1           38.     One of these facilities is Banner Lassen Medical Center in Susanville, California,  
2 originally founded in 1883, “[a] 25-bed, critical access hospital” with a “focus [] to provide you  
3 with outstanding care and an excellent patient care experience through the latest in medical  
4 technology, a vision of compassion, and a concentration on patient and employee safety [...and...]  
5 offer[ing] a wide range of programs and services to aid in prevention, diagnosis and treatment of  
6 illness.”<sup>30</sup>

7           39.     Another one of Defendant’s facilities is University Medical Center Tucson,  
8 established in 1971, a “non-profit hospital with 649 licensed beds, providing a wide range of  
9 inpatient and outpatient services [with] more than 3,000 health care professionals and support staff,  
10 and a medical staff of more than 1,300 physicians who serve Tucson and surrounding areas.”<sup>31</sup>

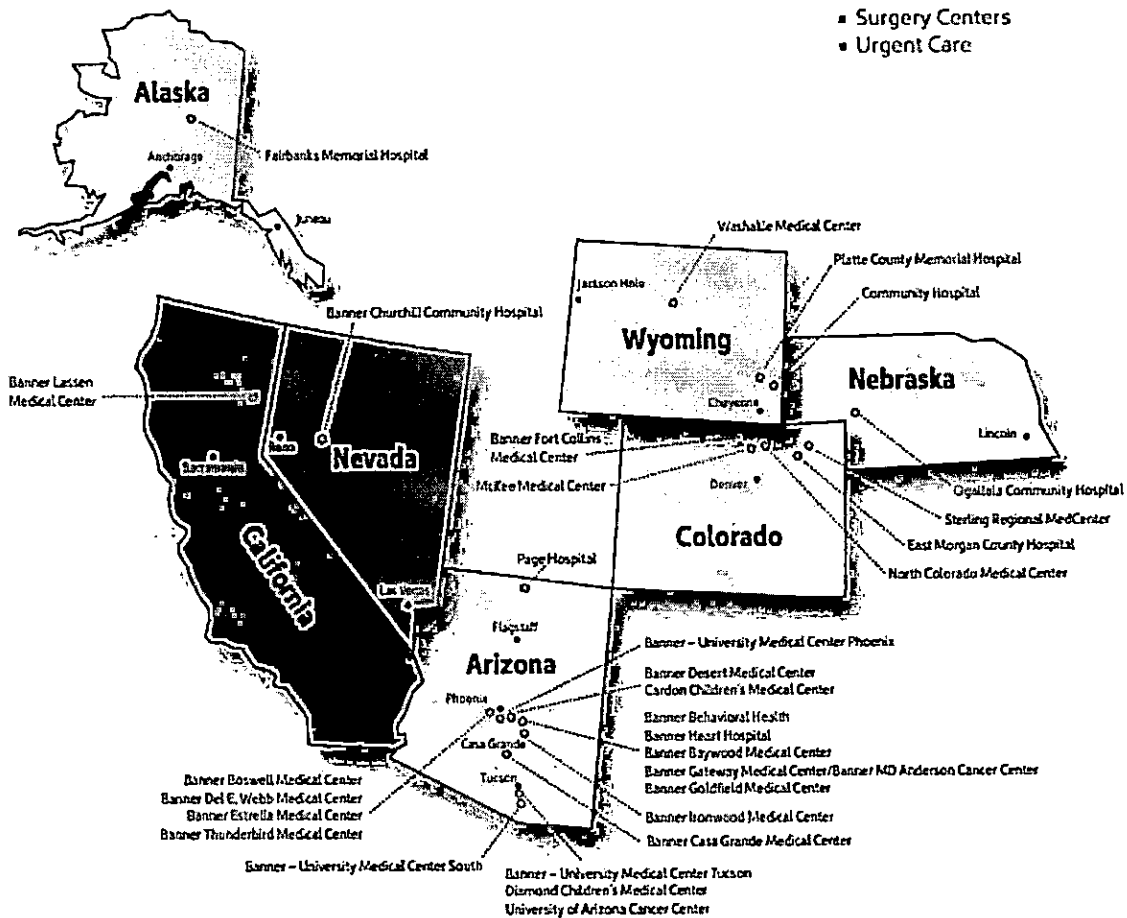
11           40.     Moreover, banner operates hundreds of physicians’ clinics, urgent care clinics,  
12 diagnostic imaging practices, physical therapy locations, surgery centers, specialized breast health  
13 centers, emergency care departments, as well as home care and equipment locations, laboratories,  
14 pharmacies, specialty care centers (e.g., Banner MD Anderson Cancer Center), and other health  
15 service locations such as Banner Health schools and senior centers.<sup>32</sup>

16  
17  
18  
19  
20 <sup>30</sup> <https://www.bannerhealth.com/locations/susanville/banner-lassen-medical-center> (last acc.  
Mar. 12, 2024).

21 <sup>31</sup> *Banner Health 2022 CHNA Banner University Medical Center – Tucson Banner University*  
22 *Medical Center – South*, adopted by Banner Health Board of Directors Dec. 9, 2022, pg. 1, avail.  
23 at <https://www.bannerhealth.com/-/media/files/project/bh/chna-reports/2022/arizona/banner-university-medical-centers-tucson-and-south-cover-section-tucson.ashx#:~:text=On%20an%20annual%20basis%2C%20Banner.65%2C000%20patients%20in%20the%20ED> (last acc. Mar. 8, 2024).

<sup>32</sup> <https://www.bannerhealth.com/find-a-location> (last acc. Mar. 8, 2024).

41. As shown on its Website, the scope of Banner's treatment is truly nationwide:<sup>33</sup>



42. At its many medical care facilities, Banner provides myriad medical treatment services, including in areas of: emergency medical care; surgery (including outpatient surgery, general surgery, and neurosurgery); Academic Medicine; Allergy & Immunology; Alzheimer's Disease & Dementia; Asthma; Audiology; Banner Brain & Spine; Bariatric & Weight Loss Surgery; Behavioral & Mental Health; Burn Care; Cancer; Concierge Medicine; Concussion; Critical Care Medicine; Dermatology; Diabetes; Doctors & Specialists; Ear, Nose & Throat;

<sup>33</sup> Banner Health, Fact Sheet, *A leading health care system in the nation*, avail. at <https://www.bannerhealth.com/-/media/files/project/bh/about/history/154267bhgeneralmainifs5115.ashx> (last acc. Mar. 8, 2024).

1 Endocrinology; Endoscopy; Eye Care; Family Medicine; Gastroenterology; Geriatrics;  
2 Gynecology; Healthy Aging; Heart; Home Care; Hospice; Imaging; Infectious Disease; Infusion  
3 Therapy; Injury Prevention; Integrative Therapy; Intensive Care; Internal Medicine; Kidney; Labs;  
4 Maternity; Medical Imaging; Neonatology; Neurology; Nutrition; Obstetrics; Occupational  
5 Health; Orthopedics; Pain Management; Palliative Care; Pediatrics; Pharmacy; Physical Therapy;  
6 Poison & Drug Information Center; Primary Care; Psychology; Pulmonary; Rehabilitation;  
7 Research; Spine; Sleep Medicine; Sports Medicine; Telehealth; Transplant; Urgent Care; Urology;  
8 Women’s Health; and Wound Care.<sup>34</sup>

9 43. Further, Banner provides specialized treatment through dedicated institutes,  
10 including: Banner - University Medicine Heart Institute (“[t]he most current and advanced care  
11 for your heart” with a Cardiovascular Intervention Center, Heart Rhythm Disorders Center, and  
12 Women’s Heart Center); Banner - University Medicine Neuroscience Institute (“State-of-the-art  
13 care for neurological conditions”); Banner - University Orthopedic and Sports Medicine Institute  
14 (“[e]xpert care to keep your muscles and joints moving”); and Banner - University Medicine  
15 Women’s Institute (“[c]omprehensive care from maternity to menopause”).<sup>35</sup>

16 44. Banner boasts having over 50,000 employees, being “one of the country’s largest  
17 employers [...], [ Arizona’s... ] largest private employer, and [ ] one of Northern Colorado’s largest  
18 employers.”<sup>36</sup>

19 45. Defendant touts that:

20 Ultimately, Banner’s unwavering commitment to the health and well-being of its  
21 communities has earned accolades from an array of industry organizations, Banner  
22 Health’s Supply Chain was recognized as second in the nation in 2021, and one of  
the nation’s Top 10 Integrated Health Systems according to SDI and Modern

23 <sup>34</sup> <https://www.bannerhealth.com/services/service-listing> (last acc. Mar. 8, 2024).

<sup>35</sup> <https://www.bannerhealth.com/services> (last acc. Mar. 8, 2024).

<sup>36</sup> <https://www.bannerhealth.com/about> (last acc. Mar. 8, 2024).

1 Healthcare Magazine. Banner Alzheimer’s Institute has also garnered international  
2 recognition for its groundbreaking Alzheimer’s Prevention Initiative, brain imaging  
3 research and patient care programs. Further, Banner Health, which is the second  
4 largest private employer in both Arizona and Northern Colorado, continues to be  
5 recognized as one of the “Best Places to Work” by Becker’s Hospital Review.<sup>37</sup>

46. In 2023, Defendant generated annual revenue approximating \$7.8 billion.<sup>38</sup>

47. Banner serves many of its patients via its Online Platforms, which it encourages  
6 patients to use to learn about Banner on its main homepage,<sup>39</sup> to search for health information,<sup>40</sup>  
7 to find a doctor,<sup>41</sup> to find locations,<sup>42</sup> to learn about medical conditions and treatment services,<sup>43</sup>  
8 to learn about classes and events,<sup>44</sup> to access a patient portal,<sup>45</sup> to pay bills,<sup>46</sup> and more.

48. In furtherance of its goal of increasing sales and profitability, and to improve the  
10 success of its advertising and marketing, Defendant purposely installed the Meta Pixel and other  
11 trackers, such as Google Analytics with Google Tag Manager (“GTM”), Facebook Events,  
12 AppDynamics, Taboola, Pinterest, StackAdapt, LinkedIn, DoubleClick, Skai, Microsoft Universal  
13 Events, and Medallia onto its Website, for the purpose of gathering information about Plaintiff and  
14 Class Members to further its marketing efforts. But Defendant did not only generate information  
15

---

16 <sup>37</sup> *Banner Health 2022 CHNA Banner University Medical Center – Tucson Banner University*  
17 *Medical Center – South*, adopted by Banner Health Board of Directors Dec. 9, 2022, pg. 1, avail.  
18 at <https://www.bannerhealth.com/-/media/files/project/bh/chna-reports/2022/arizona/banner-university-medical-centers-tucson-and-south-cover-section-tucson.ashx#:~:text=On%20an%20annual%20basis%2C%20Banner.65%2C000%20patients%20in%20the%20ED> (last acc. Mar. 8, 2024).

19 <sup>38</sup> <https://www.zippia.com/banner-health-careers-61932/revenue/> (last acc. Mar. 8, 2024).

20 <sup>39</sup> <https://www.bannerhealth.com/> (last acc. Mar. 8, 2024).

21 <sup>40</sup> E.g., search for “chest pain,” avail. at  
<https://www.bannerhealth.com/search?query=chest%20pain> (last acc. Mar. 8, 2024).

22 <sup>41</sup> <https://www.bannerhealth.com/physician-directory> (last acc. Mar. 8, 2024).

23 <sup>42</sup> <https://www.bannerhealth.com/find-a-location> (last acc. Mar. 8, 2024).

<sup>43</sup> <https://www.bannerhealth.com/services> (last acc. Mar. 8, 2024).

<sup>44</sup> <https://www.bannerhealth.com/calendar> (last acc. Mar. 8, 2024).

<sup>45</sup> [https://account.bannerhealth.com/sign-in?\\_ga=2.66854765.237380448.1709911311-131706459.1709911311](https://account.bannerhealth.com/sign-in?_ga=2.66854765.237380448.1709911311-131706459.1709911311) (last acc. Mar. 8, 2024).

<sup>46</sup> <https://bannerhealth.simplepay.com/app/login> (last acc. Mar. 8, 2024).



1 for its own use: it also shared patient information, including Private Information belonging to  
2 Plaintiff and Class Members, with Facebook and other unauthorized third parties.

3 49. To better understand Defendant's unlawful data-sharing practices, a brief  
4 discussion of basic web design and tracking tools follows.

5 *i. Facebook's Business Tools and the Meta Pixel*

6 50. Facebook operates the world's largest social media company and generated \$117  
7 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.<sup>47</sup>

8 51. In conjunction with its advertising business, Facebook encourages and promotes  
9 entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify,  
10 target, and market products and services to individuals.

11 52. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits  
12 of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby  
13 enabling the interception and collection of user activity on those platforms.

14 53. The Business Tools are automatically configured to capture "Standard Events" such  
15 as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"),  
16 as well as metadata, button clicks, and other information.<sup>48</sup> Businesses that want to target  
17 customers and advertise their services, such as Defendant, can track other user actions and can  
18

19 \_\_\_\_\_  
20 <sup>47</sup>Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK  
<https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited Nov. 14, 2022).

21 <sup>48</sup>Specifications for Facebook Pixel Standard Events, META,  
<https://www.facebook.com/business/help/402791146561655> (last visited Jan. 31, 2023); *see also*  
22 Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS;  
<https://developers.facebook.com/docs/facebook-pixel/advanced/>; *see also* Best Practices for  
23 Facebook Pixel Setup, META <https://www.facebook.com/business/help/218844828315224>; App  
Events API, META FOR DEVELOPERS, [https://developers.facebook.com/docs/marketing-api/app-  
event-api/](https://developers.facebook.com/docs/marketing-api/app-event-api/) (last visited Jan. 31, 2023).

1 create their own tracking parameters by building a “custom event.”<sup>49</sup>

2 54. One such Business Tool is the Meta Pixel, a tool that “tracks the people and type  
3 of actions they take.”<sup>50</sup> When a user accesses a webpage that is hosting the Meta Pixel, the  
4 communications with the host webpage are instantaneously and surreptitiously duplicated and sent  
5 to Facebook—traveling from the user’s browser to Facebook’s server.

6 55. Notably, this transmission only occurs on webpages that contain the Pixel. A  
7 website owner can configure its website to use the Pixel on certain webpages that don’t implicate  
8 patient privacy (such as the homepage) and disable it on pages that do implicate patient privacy  
9 (such as Defendant’s “Services” pages<sup>51</sup>).

10 56. The Meta Pixel’s primary purpose is for marketing and ad targeting and sales  
11 generation.<sup>52</sup>

12 57. Facebook’s own website informs companies that “[t]he Meta Pixel is a piece of  
13 code that you put on your website that allows you to measure the effectiveness of your advertising  
14 by understanding the actions people take on your website.”<sup>53</sup>

15 58. According to Facebook, the Meta Pixel can collect the following data.

16 **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard  
17 web protocol sent between any browser request and any server on the internet.  
18 HTTP Headers include IP addresses, information about the web browser, page  
19 location, document, referrer and *person using the website*. (emphasis added).

**Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.

20 <sup>49</sup> About Standard and Custom Website Events, META,  
21 <https://www.facebook.com/business/help/964258670337005>; *see also* Facebook, App Events  
22 API, *supra*.

<sup>50</sup> Retargeting, META, <https://www.facebook.com/business/goals/retargeting>.

23 <sup>51</sup> <https://pamhealth.com/health-services> (last acc. Mar. 6, 2024).

<sup>52</sup> *See* Meta Pixel, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/>  
(last accessed Mar. 19, 2023).

<sup>53</sup> About Meta Pixel, META,  
<https://www.facebook.com/business/help/742478679120153> (last accessed Mar. 19, 2023).

1 **Button Click Data** – Includes any buttons clicked by site visitors, the labels those  
2 buttons and any pages visited as a result of the button clicks.

3 **Optional Values** – Developers and marketers can optionally choose to send  
4 additional information about the visit through Custom Data events. Example  
5 custom data events are conversion value, page type and more.

6 **Form Field Names** – Includes website field names like email, address, quantity,  
7 etc., for when you purchase a product or service. We don't capture field values  
8 unless you include them as part of Advanced Matching or optional values.<sup>54</sup>

9 59. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- 10 • **Make sure your ads are shown to the right people.** Find new customers,  
11 or people who have visited a specific page or taken a desired action on your  
12 website.
- 13 • **Drive more sales.** Set up automatic bidding to reach people who are more  
14 likely to take an action you care about, like making a purchase.
- 15 • **Measure the results of your ads.** Better understand the impact of your ads  
16 by measuring what happens when people see them.<sup>55</sup>

17 60. Facebook likewise benefits from the data received from the Meta Pixel and uses the  
18 data to serve targeted ads and identify users to be included in such targeted ads.

19 *ii. Defendant's method of transmitting Plaintiff's and Class Members' Private*  
20 *Information via the Meta Pixel and/or Conversions API i.e., the Interplay between*  
21 *HTTP Requests and Responses, Source Code, and the Meta Pixel*

22 61. Web browsers are software applications that allow consumers to navigate the  
23 internet and view and exchange electronic information and communications. 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).

---

<sup>54</sup> Meta Pixel, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/> (last accessed Mar. 19, 2023).

<sup>55</sup> About Meta Pixel, META, <https://www.facebook.com/business/help/742478679120153> (last accessed Mar. 19, 2023).

1           62. Every website is hosted by a computer “server” that holds the website’s contents  
2 and through which the website owner exchanges files or communications with Internet users’  
3 client devices via their web browsers.

4           63. Web communications consist of HTTP Requests and HTTP Responses, and any  
5 given browsing session may consist of thousands of individual HTTP Requests and HTTP  
6 Responses, along with corresponding cookies.<sup>56</sup>

7           64. GET Requests are one of the most common types of HTTP Requests. In addition  
8 to specifying a particular URL (i.e., web address), they also send the host server data, which is  
9 embedded inside the URL and can include cookies.

10          65. When an individual visits a website, their web browser sends an HTTP Request to  
11 the entity’s servers that essentially asks the website to retrieve certain information (such as  
12 Defendant’s search function page). The entity’s servers send the HTTP Response, which contains  
13 the requested information in the form of “Markup.” This is the foundation for the pages, images,  
14 words, buttons, and other features that appear on the patient’s screen as they navigate a website.

15          66. Every website is comprised of Markup and “Source Code.” Source Code is simply  
16 a set of instructions that commands the website visitor’s browser to take certain actions when the  
17 web page first loads or when a specified event triggers the code.

18          67. Source code may also command a web browser to send data transmissions to third  
19 parties in the form of HTTP Requests quietly executed in the background without notifying the  
20 web browser’s user.

21  
22  
23 

---

<sup>56</sup>“Cookies are small files of information that a web server generates and sends to a web browser . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience.” <https://www.cloudflare.com/learning/privacy/what-are-cookies/> (last visited Jan. 27, 2023).

1           68. Defendant’s implementation of the Meta Pixel is source code that acted much like  
2 a traditional wiretap, intercepting and transmitting communications intended only for Defendant.

3           69. Separate from the Meta Pixel, Facebook and other website owners can place third-  
4 party cookies in the web browsers of users logged into their websites or services. These cookies  
5 can uniquely identify the user so the cookie owner can track the user as he moves around the  
6 internet—whether on the cookie owner’s website or not. Facebook uses this type of third-party  
7 cookie when Facebook account holders use the Facebook app or website. As a result, when a  
8 Facebook account holder uses Defendant’s Website, the account holder’s unique Facebook ID is  
9 sent to Facebook, along with the intercepted communication, allowing Facebook to identify the  
10 patient associated with the Private Information it has intercepted.

11           70. With substantial work and technical know-how, internet users can sometimes  
12 circumvent this browser-based wiretap technology. To counteract this, third parties bent on  
13 gathering data and Private Information implement workarounds that are difficult to detect or evade.  
14 Facebook’s workaround is its Conversions API tool, which is particularly effective because the  
15 data transmitted via this tool does not rely on the website visitor’s web browsers. Rather, the  
16 information travels directly from the entity’s server to Facebook’s server.

17           71. Conversions API “is designed to create a direct connection between [web hosts’]  
18 marketing data and [Facebook].”<sup>57</sup> Thus, the entity receives and stores its communications with  
19 patients on its server before Conversions API collects and sends those communications—and the  
20 Private Information contained therein—to Facebook.

21           72. Notably, client devices do not have access to host servers and thus cannot prevent  
22  
23

---

<sup>57</sup> About Conversions API, META, <https://www.facebook.com/business/help/2041148702652965> (last visited May 15, 2023).

1 (or even detect) this additional transmission of information to Facebook.

2 73. While there is no way to confirm with certainty that a website owner is using  
3 Conversions API without accessing the host server, Facebook instructs companies like Defendant  
4 to “[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both  
5 tools,” because such a “redundant event setup” allows the entity “to share website events [with  
6 Facebook] that the pixel may lose.”<sup>58</sup> Thus, if an entity implemented the Meta Pixel in accordance  
7 with Facebook’s documentation, it is also reasonable to infer that it implemented the Conversions  
8 API tool on its Website.

9 74. The third parties to whom a website transmits data through pixels and other tracking  
10 technology do not provide any substantive content on the host website. In other words, Facebook  
11 and others like it are not providing anything to the user relating to the user’s communications.  
12 Instead, these third parties are typically procured to track user data and communications only to  
13 serve the marketing purposes of the website owner (i.e., to bolster profits).

14 75. Accordingly, without any knowledge, authorization, or action by a user, a website  
15 owner like Defendant can use its source code to commandeer its patients’ computing devices,  
16 causing the device’s web browser to contemporaneously and invisibly re-direct the patients’  
17 communications to hidden third parties like Facebook.

18 76. In this case, Defendant employed the Meta Pixel and potentially Conversions API  
19 to intercept, duplicate, and re-direct Plaintiff’s and Class Members’ Private Information to  
20 Facebook contemporaneously, invisibly, and without the patient’s knowledge.

21  
22  
23  

---

<sup>58</sup> See Best Practices for Conversions API, META,  
<https://www.facebook.com/business/help/308855623839366> (last visited May 15, 2023).

1 77. Consequently, when Plaintiff and Class Members visited Defendant's Website and  
2 communicated their Private Information, it was simultaneously intercepted and transmitted to  
3 Facebook.

4 78. On information and belief, Banner also employed other trackers, such Google  
5 Analytics with Google Tag Manager ("GTM"), Facebook Events, AppDynamics, Taboola,  
6 Pinterest, StackAdapt, LinkedIn, DoubleClick, Skai, Microsoft Universal Events, and Medallia,  
7 which likewise transmitted Plaintiff's and the Class Members' Private Information to third parties  
8 without Plaintiff's and Class Members' knowledge or authorization.

9 *iii. Defendant Violated its own Privacy Policies*

10 79. Banner maintains and is covered under privacy policies, including a Notice of  
11 Privacy Practices,<sup>59</sup> a Website Privacy Statement,<sup>60</sup> and a Website Terms of Use,<sup>61</sup> which are  
12 posted on Defendant's Website (collectively "Privacy Policies").

13 80. In its Notice of Privacy Practices, Defendant represents, acknowledges, and  
14 promises:

15 **Banner is committed to protecting the confidentiality of information about you**  
16 **and is required by law to do so.** This notice describes how we may use  
17 information about you within Banner Health and how we may disclose it to others  
18 outside Banner. **We will notify you if there is a breach of your unsecured**  
19 **protected health information.** This notice also describes the rights you have  
20 concerning your own health information.<sup>62</sup>

20 <sup>59</sup> Banner Health, *Notice of Privacy Practices*, effective date September 23, 2023, available at  
21 <https://www.bannerhealth.com/-/media/files/project/bh/patients-visitors/privacy-practices/hipaa-eng-fs-03-28-19.ashx> (last acc. Mar. 8, 2024), **attached as Exhibit B.**

22 <sup>60</sup> Banner Health, *Privacy Statement*, last updated November 2019, avail. at  
23 <https://www.bannerhealth.com/about/legal/notices/privacy> (last acc. Mar. 8, 2024), **attached as Exhibit C.**

<sup>61</sup> Banner Health, *Terms of Use*, avail. at <https://www.bannerhealth.com/about/legal-notices/terms> (last acc. Mar. 8, 2024), **attached as Exhibit D.**

<sup>62</sup> *Notice of Privacy Practices, Exhibit B* (emphases added).

1           81.     Therein, Banner further specifically represents, acknowledges, and promises that  
2 except as provided in the Notice of Privacy Practices, “[o]ther uses and disclosures not  
3 described in this notice will be made only with your written authorization, such as sale of  
4 medical information. You may revoke such an authorization by sending us a written request.”<sup>63</sup>

5           82.     Indeed, Banner’s Notice of Privacy Practices enumerates specific purposes for  
6 which it may disclose PHI/Private Information, including for: treatment (“Banner may use  
7 information about you to provide you with medical services and supplies. We may also disclose  
8 information about you to others that need the information to treat you, such as doctors, physician  
9 assistants, nurses, medical and nursing students, technicians, therapists, emergency service and  
10 medical transportation providers, medical equipment providers, and others involved in your  
11 care.”); in a Facility Directory; to family members and others involved in patient care; to effectuate  
12 payment for services; for health care operations (“Banner may use and disclose information about  
13 you if it is necessary to improve the quality of care we provide to patients or for health care  
14 operations. We may use information about you to conduct quality improvement activities, to obtain  
15 audit, accounting, or legal services, or to conduct business management and planning. For  
16 example, we may use medical information to review our treatment and services and to evaluate  
17 the performance of our staff in caring for you.”); for fundraising; for research; as required by law  
18 (“Federal, state, or local laws do not require patient consent to disclose information that is required  
19 to be reported. For instance, we are required to report child abuse and neglect, gunshot wounds,  
20 etc. Public policy has determined that these types of needs outweigh the patient’s right to privacy.  
21 Banner is also required to give information to the state workers’ compensation program for work-  
22 related injuries.”); for public health purposes; in limited circumstances for public safety; in

---

23 <sup>63</sup> *Id.* (bold emphasis added).



1 connection with Health Oversight Activities; to coroners, medical examiners, and funeral  
2 directors; in connection with organ and tissue donations; for military veterans, national security,  
3 and other government purposes; and in judicial proceedings, subject to certain requirements.<sup>64</sup>

4 83. None of the above purposes enumerated in Banner's Notice of Privacy Practices,  
5 for which it may disclose patients' health information/PHI/Private Information without written  
6 authorization, include Defendant disclosing that information to third-parties uninvolved in their  
7 treatment for marketing purposes.

8 84. Further, Defendant maintains a Privacy Statement, applicable to its Website, in  
9 which Banner states is applicable:

10 ... to the information we collect from you when you use voice, mobile device and  
11 desktop Banner Health platforms, tools and applications, BannerHealth.com and  
12 other Banner Health websites (collectively the "Services"), how we use that  
13 information, and when we disclose it. It will also give you more information about  
14 how to manage the personal information that you provide to us through the  
15 Services. This statement applies only to information you provide to us online while  
16 visiting or using our Services. It does not apply to information we have obtained or  
17 may obtain offline through other traditional means.<sup>65</sup>

18 85. In its Website Privacy Statement, Banner explains the information it collects from  
19 the Online Platforms, including "Automatically Collected Information" or "information []  
20 automatically received and sometimes collected from you when you use the Services [...]  
21 includ[ing] some or all of the following items: the name of the domain and host from which you  
22 access the Internet, including the Internet protocol (IP) address of the computer you are using and  
23 the IP address of your Internet Service Provider; the type and version of Internet browser software  
you use and your operating system; the type and version of your media player(s); the date and time  
you access our Services, the length of your stay and the specific pages, images, video or forms that

---

<sup>64</sup> *Id.*

<sup>65</sup> *Privacy Statement, Exhibit C.*

1 you access while using the Services; the Internet address of the website from which you linked  
2 directly to our Services and, if applicable, the search engine that referred you and any search strings  
3 or phrases that you entered into the search engine to find the Services; and demographic  
4 information concerning the country of origin of your computer and the language(s) used by it.”<sup>66</sup>

5 86. Further, therein, Banner explains that it collects information via cookies, stating:

6 "Cookies" are small files or records that we place on your computer's hard drive to  
7 distinguish you from other visitors using the Services. The use of cookies is a  
8 standard practice among websites to collect or track information about your  
9 activities while using the Services. Some websites use persistent cookies, which are  
10 placed on your computer and remain there until you delete them. Others use  
11 temporary cookies, which expire after some period or become overwritten by other  
12 data. **Banner Health Services use "session cookies" which disappear from your  
13 computer after you have closed your Internet browser.**

14 Most people do not know that cookies are being placed on their computers when  
15 they use Banner Health Services or most other websites because browsers are  
16 typically set to accept cookies. You can choose to have your browser warn you  
17 every time a cookie is being sent to you or you can turn off cookie placements. If  
18 you refuse cookies, you can still use Banner Health Services, but your overall  
19 experience may be affected and some functionality may be reduced or  
20 unavailable.<sup>67</sup>

21 87. Lastly, in the Privacy Statement, Defendant explains that it collects information  
22 Website users actively submit when they “(i) submit a job application; (ii) make an online  
23 donation; (iii) sign up for a class or event conducted at one of our medical centers; (iv) send an e-  
mail message to us or otherwise provide online comments, criticisms, suggestions or feedback; (v)  
participate in a chat session; (vi) purchase merchandise from the Banner Store; (vii) reserve a spot  
or make an appointment at a Banner Health facility; or (viii) pre-register for a hospital procedure  
such as surgery.”<sup>68</sup>

---

23 <sup>66</sup> *Id.*

<sup>67</sup> *Id.* (bold emphasis added).

<sup>68</sup> *Id.*

1           88. In its Privacy Statement, Defendant specifically delineates how it uses and shares  
2 Private Information, *to wit*:

- 3           • To process, complete or otherwise act upon or respond to your  
4 request or reason for submitting that information;
- 5           • To register and/or verify you in connection with a service or feature  
6 that you are attempting to access or obtain;
- 7           • To communicate with you about your request or reason for  
8 submitting that information;
- 9           • To provide additional information to you about Banner Health and  
10 its services that we believe may interest you;
- 11           • To study and analyze the use of the information and features  
12 available on our Services; and
- 13           • To assist, when necessary, in protecting our rights or property,  
14 enforcing the provisions of our Privacy Statement and Terms of Use,  
15 and/or preventing harm to you or others.<sup>69</sup>

16           89. None of the above-described purposes enumerated in Banner’s Privacy Statement  
17 include the disclosure of Private Information to third parties uninvolved in patients’ treatment for  
18 marketing purposes, without their authorization, as occurred in the Disclosure.

19           90. Moreover, in its Privacy Statement, Defendant specifically represents,  
20 acknowledges, and promises that, “*We do not sell User Information to third parties.* And except  
21 where we otherwise obtain your express permission, we share your User Information with third  
22 parties only under the limited circumstances stated, including: credit card authorizations, “to  
23 process a particular request you have made, to complete a purchase order for merchandise and to  
deliver your purchase to you or to process a donation[;]” “[...]to conduct background checks,  
obtain credit reports, verify prior employment, check references and for any other lawful purpose  
that is in our judgment reasonably necessary to our interviewing and hiring process; “...in response  
to judicial or other governmental subpoenas, warrants and court orders served on Banner Health

---

<sup>69</sup> *Id.*

1 in accordance with their terms, or as otherwise required by applicable law[;]" "to protect our rights  
2 or property, to enforce the provisions of our Privacy Statement and Terms of Use, and/or to prevent  
3 harm to you or others[;]" "...if Banner Health or its business is sold or offered for sale to another  
4 company or person(s), if a petition for relief under the United States Bankruptcy Laws is filed by  
5 or against Banner Health, or if Banner Health becomes subject to an order of appointment of a  
6 trustee or receiver[;]" and sharing user correspondence and information provided in user emails  
7 "with employees, volunteers, representatives, or agents most capable of addressing your  
8 correspondence" if users communicate via email.<sup>70</sup>

9 91. Nothing in Defendant's Website Privacy Statement discloses Banner's use of the  
10 Meta Pixel or related tracking technology, and that users' and patients' Private Information will  
11 be disclosed to third parties uninvolved in patient's treatment, without their authorization.

12 92. Finally, Defendant maintains a Website Terms of Use, which states, "[b]y  
13 accessing, using or downloading in any way, without limitation, any materials from this Website  
14 or merely browsing this Website, you agree to and are bound by these Terms of Use."<sup>71</sup>

15 93. Banner's Website Terms of Use provides:

16 **Banner Health respects the privacy of visitors to our Website. Please see**  
17 **Banner Health's Privacy Statement relating to the collection and use of your**  
18 **information. User acknowledges and agrees that this Privacy Statement,**  
19 **including but not limited to the manner that Banner Health collects, uses and**  
20 **discloses User's personally identifiable information, is incorporated and made**  
21 **part of these Terms of Use. If User does not agree to Banner Health's Privacy**  
22 **Statement, then User should not use this Website or submit or post any personally**  
23 **identifiable information on this Website. Questions regarding privacy issues should**  
**be directed to Banner Health System Web Services.**<sup>72</sup>

---

<sup>70</sup> *Id.* (italics in original).

<sup>71</sup> *Terms of Use, Exhibit D.*

<sup>72</sup> *Id.* (bold emphasis added).

1           94. In addition, in its Website Terms of Use, Banner “reserves the right to monitor all  
2 network traffic to this Website to identify and/or block unauthorized attempts or intrusions to  
3 upload or change information or cause damage to this Website in any fashion. Anyone using this  
4 Website expressly consents to such monitoring.”<sup>73</sup>

5           95. Nothing in the Website Terms of Use discloses Banner’s use of the Meta Pixel or  
6 related tracking technology, and that users’ and patients’ Private Information will be disclosed to  
7 third parties uninvolved in patient’s treatment, without their authorization.

8           96. Despite these express, specific representations and promises in its Privacy Policies,  
9 Banner does indeed transfer Private Information to third parties. Using the Meta Pixel, Defendant  
10 used and disclosed Plaintiff’s and Class Member’s Private Information and confidential  
11 communications to Facebook, and other unauthorized third parties, without written authorization,  
12 in violation of Banner’s Privacy Policies.

13           ***iv. Banner Unauthorizedly Disclosed Plaintiff’s and the Class’s Private Information***

14           97. Defendant disclosed Plaintiff’s and Class Members’ Private Information and  
15 confidential communications to third parties for marketing purposes, including Facebook, and  
16 potentially others, including Google Analytics with Google Tag Manager (“GTM”),  
17 AppDynamics, Taboola, Pinterest, StackAdapt, LinkedIn, Skai, Microsoft Universal Events, and  
18 Medallia, without Plaintiff’s and Class Members’ authorization.

19           98. Through its use of the Meta Pixel, Banner disclosed to Facebook Plaintiff’s and  
20 Class Members’ Private Information communicated via its Website, including details about the  
21 pages they browsed and the buttons they clicked, including (i) users’ keyword searches, (ii) users’  
22 physician searches, (iii) content that users viewed, and (iv) activities that reveal the users’ status  
23

---


<sup>73</sup> *Id.*

1 as potential patients.

2 99. In addition to this information, (v) the Meta Pixel collects and transmits to  
3 Facebook other identifying information, including IP addresses, and users' "c\_user" cookies,  
4 which Facebook uses to identify users, and are transmitted in Meta Pixel events. Therefore, the  
5 Meta Pixel events Banner sent likely allowed Facebook to connect users' identities with the details  
6 reported within the events.

7 100. For example, Banner installed Meta Pixels on its pages for medical services:<sup>74</sup>


8 3/22/23, 10:47 AM


9  **Meta Pixel Helper**  
10 Learn More

---

11 6 pixel found on [www.bannerhealth.com](http://www.bannerhealth.com)

---

12  **Meta Pixel** Troubleshoot Pixel  
13 Pixel ID: 134130160733505 [click to copy](#) Set Up Events New!

14 ▼  PageView View Analytics

15 **EVENT INFO**

16 Setup Method: Manual  
17 URL called: Hide

18 `https://www.facebook.com/tr?id=134130160733505&ev=PageView&dl=https%3A%2F%2Fwww.bannerhealth.com%2Fservices&rl=https%3A%2F%2Fwww.bannerhealth.com%2F&if=false&ts=1679499816849&sw=1920&sh=1080&v=2.9.99&r=stable&ec=0&o=28&CS_est=true&fbp=fb.1.167949986115.867806339&ic=fbpixel&it=1679499816146&coo=false&rqm=GET`

19 Load Time: 8.30 ms  
20 Pixel Code: Hide

21 `<noscript></noscript>`

22 Pixel Location: Hide  
`https://www.bannerhealth.com/services`

23 Frame: Window

<sup>74</sup> <https://www.bannerhealth.com/services> (last acc. Mar. 8, 2024).

1 101. As of October 2023, Banner had multiple Meta Pixels installed on its Website with  
2 the following IDs: 534707753606264 (“Pixel1”); 354902315267014 (“Pixel2”);  
3 876783143355083 (“Pixel3”); 317691905318614 (“Pixel4”); 134130160733505 (“Pixel5”); and  
4 352572695583032 (“Pixel6”).

5 102. Even prior to that time, as of March 30, 2021, Banner had three additional Meta  
6 Pixels with IDs: 200525233628970 (“Pixel7”); 375127919853316 (“Pixel8”); and (9)  
7 499798837564477 (“Pixel9”). Further, there are three GTM accounts with IDs GTM-P6NQWFD  
8 (“GTM1”), GTM-K8Z9P6T (“GTM2”), and GTM-NSPWG36 (“GTM3”).

9 Banner Disclosed Users’ Keyword Searches

10 103. Banner shared information with Facebook about users’ searches through  
11 PageView, Microdata, and SubscribedButtonClick events.

12 104. Upon users’ arrival on Banner’s homepage, Banner sent PageView and Microdata  
13 events informing Facebook that the user was on “.” The Microdata event also provides that Banner  
14 offers healthcare in “AZ, CO, WY, NE, NV, CA” and that the user can “Find a provider, schedule  
15 an appointment, or find the nearest Banner Health location near you.”

16 105. As users moved beyond the homepage, Banner continued to report users’ activities  
17 to Facebook.

18 106. If that was not bad enough, Defendant sent Facebook Plaintiff’s and the Class  
19 Members’ search query information. For example, when a user searched for the keyword “cancer,”  
20 Banner reported that activity to Facebook through SubscribedButtonClick, PageView and  
21 Microdata events, which all disclosed the user’s “query=cancer.”

22 107. The SubscribedButtonClick event includes additional information about the user’s  
23 specific activities, such as that the user clicked a button labeled “Search” connected to a form that

1 allows the user to “Search for doctors, locations, services, and more.”

2 108. With the search results displayed, the user may refine their search results by  
3 displaying the results by categories such as all results, locations results, or services results only.  
4 Banner also reported this type of activity. For example, if the user clicked to display all results,  
5 Banner sent a SubscribedButtonClick event, revealing that the user clicked on a button labeled  
6 “SERVICES” on a page titled “Banner Health Search Results” and that the user navigated to that  
7 page by searching “query=cancer.”

8 Banner Disclosed Users’ Physician Search Activities

9 109. Banner informed Facebook when users searched for physicians on the Banner  
10 website through SubscribedButtonClick, PageView, and Microdata events.

11 110. Banner sent a SubscribedButtonClick event as soon as a user navigated to Banner’s  
12 Find A Doctor page.

13 111. The SubscribedButtonClick disclosed that the user clicked a button labeled “Find a  
14 Doctor” and that the user navigated to the user’s current page after viewing a page on  
15 “<https://www.bannerhealth.com/services/cancer>.”

16 112. Upon the user loading the Find a Doctor page, Banner sent a pair of PageView and  
17 Microdata events, confirming that the user landed on the page with a “physician-directory” for the  
18 user to “Find a Doctor near you.”

19 113. Finally, as the user clicked to search for an oncology physician, Banner sent another  
20 SubscribedButtonClick event, informing Facebook that the user clicked “Search” to “Find a  
21 Doctor.”

22

23



Banner Disclosed Content That Users Viewed

1  
2 114. Additionally, Defendant shared information as to the contents of its Website pages  
3 which Website users viewed. Banner disclosed information about content that users viewed  
4 through PageView, Microdata, and SubscribedButtonClick events.

5 115. For instance, when a user clicked to view “Classes + Events,” Banner reported that  
6 via a SubscribedButtonClick event. When the user arrived on Banner’s calendar page for its classes  
7 and events, Banner sent a pair of PageView and Microdata events, disclosing that the user was  
8 looking at the “/calendar” page.

9 116. Banner continued to share the user’s activities as the user clicked on specific  
10 classes. For instance, when the user clicked to view more about a diabetes class, Banner reported  
11 that the user clicked a button labeled “Dial Into Diabetes: Nutrition Basics and Medication  
12 Management- Virtual” while the user was on the “Calendar” page.

13 117. When the Dial Into Diabetes information page loaded, Banner sent another pair of  
14 PageView and Microdata events. The Microdata event reveals the user’s potential health insurance  
15 status due to the fact that the event indicates the user must be insured by “Banner Medicare  
16 Advantage (Dual, HMO, PPO) in order to register for the class.”

17 118. Additionally, the Microdata event reveals more information about the Dial Into  
18 Diabetes class too, including the time and date of the event, e.g., “11/01/2023, 10:00 am,” and the  
19 modality of the class via “Microsoft Teams Meeting.”

20 119. Then, Banner disclosed the user’s registration for the class through a series of  
21 SubscribedButtonClick, PageView, and Microdata events.

22 120. As another illustration of Banner’s disclosures of content that users viewed, Banner  
23 transmitted a series of SubscribedButtonClick, PageView, and Microdata events as the user took

1 a heart health risk assessment on Banner's website.

2 121. Banner began reporting about the user's health risk assessment activities when the  
3 user clicked to view Banner's offered health risk assessments. As the user clicked to browse the  
4 offered assessments, Banner sent a SubscribedButtonClick event.

5 122. When the page loaded, Banner then sent a pair of PageView and Microdata events,  
6 informing Facebook that the user can take "free health risk assessments" to "learn about your risk  
7 as well as stay informed about your health."

8 123. Next, when the user loaded a page for the heart health risk assessment, Banner  
9 transmitted PageView and Microdata events, revealing that the user was viewing a "Heart Age  
10 Test" which allows the user to "Estimate your risk of heart and blood vessel disease."

11 124. As the user clicked to start the assessment, progressed through each question, and  
12 then completed the assessment, Banner sent a mixture of SubscribedButtonClick, Pageview, and  
13 Microdata events sharing the user's progress with Facebook.

14 Banner Discloses Users' Activities That Reveal Their Status as Potential Patients

15 125. Further still, Banner discloses Users' activities that reveal their status as potential  
16 patients. Through PageView, Microdata, and SubscribedButtonClick events, Banner disclosed  
17 information about users' activities that reveal their status as potential patients.

18 126. For example, when the user clicked to access the Patient Account page, Banner sent  
19 a SubscribedButtonClick event disclosing that the user clicked a button labeled "Patient Account"  
20 on a page titled "Patients & Visitors | Banner Health." Banner further sent PageView and  
21 Microdata events, informing Facebook that the user was now on the Patient Account page, which  
22 "offers 24/7 online access to your health information."

23 127. From the Patient Account page, the user could either click to create a patient

1 account or click to sign into their patient account. Both activities triggered a  
2 SubscribedButtonClick event, disclosing that the user was on the “/patient-account” page and that,  
3 either, the user clicked a button for “Creating an Account” or to “Sign In,” respectively.

4 128. In addition to Banner sharing information with Facebook about users’ patient  
5 account-related activities, Banner also sent events with data about users’ activities related to  
6 medical records.

7 129. As a user navigated to Banner’s page for patients and then to a subpage for medical  
8 records, Banner sent a series of SubscribedButtonClick, PageView, and Microdata events  
9 informing Facebook about those activities. The Microdata events reveal information about the  
10 pages that the user was viewing. For example, the Microdata event associated with the Patient page  
11 reveal that the page the user was viewing offered “resources . . . to make your patient visit or stay  
12 at a Banner Health location as comfortable and successful as possible.”

13 130. Similarly, the Microdata event for the Medical Records page disclose that users  
14 “can request copies of your medical record information” from Banner.

15 131. Moreover, Banner also disclosed information about users’ interactions related to  
16 medical bills. Upon the user clicking a button to open and loading a page about payment options  
17 and other billing information, Banner sent SubscribedButtonClick, PageView, and Microdata  
18 events, disclosing that the user clicked on a button to access Banner’s “patients/billing” page where  
19 they could “Learn more about the financial assistance programs, pricing, insurance information,  
20 programs and policies available for you at Banner Health.”

21 132. From Banner’s Billing page, the user had the option to pay their bill for services  
22 received from Banner’s various service centers: (i) the imaging section, (ii) the surgery center,  
23 (iii) urgent care unit, or (iv) the Wyoming Medical Center.

1           133. As the user clicked to pay their bill for imaging services, surgery center services,  
2 urgent care services, or Wyoming Medical Center services, Banner sent a SubscribedButtonClick  
3 event informing Facebook that the user clicked on a button labeled “Imaging online payment,”  
4 “Surgery Center online payment,” “Urgent Care online payment,” or “Wyoming Medical Center  
5 online payment,” respectively.

6           134. After the pages for the different Banner service centers loaded, Banner also sent a  
7 pair of PageView and Microdata events, each of which revealed additional data about the pages  
8 that the user was viewing. For instance, the Microdata event sent for the surgery center page  
9 informed Facebook that the user was viewing a page that was “Your one-stop shop for all Banner  
10 Surgery Center payment processes.”

11           135. When the user proceeded to pay, for example, on the urgent care billing page,  
12 Banner disclosed that activity as well through a SubscribedButtonClick event.

13           136. Banner also disclosed when the user loaded the login page for Wyoming Medical  
14 Center through a PageView event.

15                           Banner Discloses Users’ Identifying Information

16           137. In addition, as noted, the Meta Pixel collects and transmits to Facebook other  
17 identifying information, including Users’ IP addresses, and users’ “c\_user” cookies, which  
18 Facebook uses to identify users.

19           138. Therefore, the Meta Pixel events Banner sent likely allowed Facebook to connect  
20 users’ identities with the details reported within the events.

21           139. After receiving this information from Defendant, Facebook processes it, analyzes  
22 it, and assimilates it into its own massive datasets, before selling access to this data in the form of  
23 targeted advertisements. Employing “Audiences”—subsections of individuals identified as

1 sharing common traits—Facebook promises the ability to “find the people most likely to respond  
2 to your ad.”<sup>75</sup> Advertisers can purchase the ability to target their ads based on a variety of criteria:  
3 “Core Audiences,” individuals who share a location, age, gender, and/or language;<sup>76</sup> “Custom  
4 Audiences,” individuals who have taken a certain action, such as visiting a website, using an app,  
5 or buying a product bought a product;<sup>77</sup> and/or “Lookalike Audiences,” groups of individuals who  
6 “resemble” a Custom Audience, and who, as Facebook promises, “are likely to be interested in  
7 your business because they’re similar to your best existing customers.”<sup>78</sup>

8 140. Google and other companies process data in a similar manner and use it to build  
9 marketing and other data profiles allowing for targeted advertising.

10 141. Defendant could have chosen not to use the Meta Pixel, or it could have configured  
11 it to limit the information that it communicated to third parties, but it did not. Instead, it  
12 intentionally selected and took advantage of the features and functionality of the Pixel that resulted  
13 in the Disclosure of Plaintiff’s and Class Members’ Private Information.

14 142. Along those same lines, Defendant could have chosen not to use other tracking  
15 technologies such as, Google Analytics with Google Tag Manager (“GTM”), Facebook Events,  
16 AppDynamics, Taboola, Pinterest, StackAdapt, LinkedIn, DoubleClick, Skai, Microsoft Universal  
17 Events, and Medallia to track Plaintiff and Class Members private communications and transmit  
18 that information to unauthorized third parties. It did so anyway, intentionally taking advantage of  
19 these trackers despite the harm to Plaintiff’s and Class Members’ privacy.

21 \_\_\_\_\_  
22 <sup>75</sup> Audience Ad Targeting, Meta, <https://www.facebook.com/business/ads/ad-targeting> (last  
23 visited Aug. 14, 2023).

<sup>76</sup> *Id.*

<sup>77</sup> *Id.*

<sup>78</sup> How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Help Center,  
<https://www.facebook.com/business/help/465262276878947> (last visited Aug. 14, 2023).

1           143. Defendant used and disclosed Plaintiff's and Class Members' Private Information  
2 to Facebook, and possibly other third parties, for the purpose of marketing their services and  
3 increasing its profits.

4           144. On information and belief, Defendant shared, traded, or sold Plaintiff's and Class  
5 Members' Private Information with Facebook, and potentially other third parties, in exchange for  
6 improved targeting and marketing services.

7           145. Plaintiff and the Class Members never consented, agreed, authorized, or otherwise  
8 permitted Defendant Banner to intercept their communications or to use or disclose their Private  
9 Information for marketing purposes. Plaintiff and the Class were never provided with any written  
10 notice that Defendant disclosed its patients' Protected Health Information to Facebook and others,  
11 nor were they provided any means of opting out of such disclosures. Defendant nonetheless  
12 knowingly disclosed Plaintiff's and the Class's Protected Health Information to unauthorized  
13 entities.

14           146. Plaintiff and Class Members relied on Defendant to keep their Private Information  
15 confidential and securely maintained, to use this information for legitimate healthcare purposes  
16 only, and to make only authorized disclosures of this information.

17           147. Furthermore, Defendant actively misrepresented that it would preserve the security  
18 and privacy of Plaintiff's and Class Members' Private Information. In actuality, Defendant shared  
19 data about Plaintiff's and Class Members' activities on the Online Platforms alongside identifying  
20 details about the Plaintiff and Class Members, such as their IP addresses.

21           148. By law, Plaintiff and the Class Members are entitled to privacy in their Protected  
22 Health Information and confidential communications. Banner deprived Plaintiff and Class  
23 Members of their privacy rights when it (1) implemented a system that surreptitiously tracked,

1 recorded, and disclosed Plaintiff's and Class Members' confidential communications, Personally  
2 Identifiable Information, and Protected Health Information; (2) disclosed patients' Private  
3 Information to unauthorized, third-party eavesdroppers, including Facebook and possibly others;  
4 and (3) undertook this pattern of conduct without notifying Plaintiff and Class Members and  
5 without obtaining their express written consent.

6 **B. Plaintiff's Experience**

7 149. Plaintiff has been a patient of Defendant since 2008, approximately, receiving  
8 healthcare services from Banner and physicians in Banner's network, including for spinal  
9 degeneration at Banner Lassen Medical Center in Susanville, California.

10 150. Plaintiff relied on Banner's Website and Online Platforms to communicate  
11 confidential patient information, beginning in 2021 using personal computing devices in Lassen  
12 County, and last in October 2023. Specifically, he used the Website's search function to search  
13 for health information on spinal degeneration, and to search for physicians;<sup>79</sup> used the Website's  
14 find a doctor function;<sup>80</sup> used the patient account and/or patient portal, including to make medical  
15 appointments, check laboratory results, and make recurring payments of bills for services.<sup>81</sup>

16 151. Plaintiff accessed Defendant's Website and Online Platforms at Defendant's  
17 direction and encouragement. Plaintiff reasonably expected that his communications with Banner  
18 were confidential, solely between himself and Banner, and that, as such, those communications  
19 would not be transmitted to or intercepted by a third party.

20 152. Plaintiff provided his Private Information to Defendant and trusted that the  
21

22 <sup>79</sup> E.g., search for "chest pain," avail. at  
<https://www.bannerhealth.com/search?query=chest%20pain> (last acc. Mar. 8, 2024).

23 <sup>80</sup> <https://www.bannerhealth.com/physician-directory> (last acc. Mar. 8, 2024).

<sup>81</sup> [https://account.bannerhealth.com/sign-in?\\_ga=2.66854765.237380448.1709911311-131706459.1709911311](https://account.bannerhealth.com/sign-in?_ga=2.66854765.237380448.1709911311-131706459.1709911311) (last acc. Mar. 8, 2024).

1 information would be safeguarded according to Banner's Privacy Policies and the law.

2 153. On information and belief, through its use of the Meta Pixel on the Website and  
3 Online Platforms, Defendant disclosed to Facebook:

- 4 a. Plaintiff's identity via his IP addresses and/or "c\_user" cookies;
- 5 b. Plaintiff's seeking of medical treatment;
- 6 c. Plaintiff's status as a patient;
- 7 d. Plaintiff's search terms and activities, including relating to his health  
8 information and diagnoses, and doctors;
- 9 e. The doctors Plaintiff searched for and viewed;
- 10 f. The pages and content Plaintiff viewed; and,
- 11 g. Plaintiff's activity on the patient account and/or patient portal, including the  
12 appointments he scheduled, his laboratory results, and bills he paid.

13 154. By failing to receive the requisite consent, Banner breached confidentiality and  
14 unlawfully disclosed Plaintiff's Private Information.

15 155. Plaintiff first discovered that Defendant was using the Meta Pixel and other tracking  
16 technologies to gather and disclose his Private Information in October of 2023.

17 156. As a result of Banner's Disclosure of Plaintiff's Private Information via the Meta  
18 Pixel and other tracking technologies to third parties without authorization, Plaintiff now receives  
19 targeted health-related advertisements relating to spinal degeneration and having a newborn baby,  
20 reflecting his private medical treatment information.

21 157. Plaintiff paid Banner for medical services and the services he paid for included  
22 reasonable privacy and data security protections for his Private Information, but Plaintiff did not  
23 receive the privacy and security protections for which he paid, due to Defendant's Disclosure.



1 158. Because of Defendant's unauthorized Disclosure of his Private Information,  
2 Plaintiff has suffered injuries, including monetary damages; loss of privacy; unauthorized  
3 disclosure of this Private Information; unauthorized access to his Private Information by third  
4 parties; use of the Private Information for advertising purposes; embarrassment, humiliation,  
5 frustration, and emotional distress; decreased value of his Private Information; lost benefit of the  
6 bargain; and increased risk of future harm resulting from further unauthorized use and disclosure  
7 of his information.

8 **C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI**

9 159. In June 2020, after promising users that app developers would not have access to  
10 data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party  
11 developers to access this data.<sup>82</sup> This failure to protect users' data enabled thousands of developers  
12 to see data on inactive users' accounts if those users were Facebook friends with someone who  
13 was an active user.

14 160. On February 18, 2021, the New York State Department of Financial Services  
15 released a report detailing the significant privacy concerns associated with Facebook's data  
16 collection practices, including the collection of health data. The report noted that while Facebook  
17 maintained a policy that instructed developers not to transmit sensitive medical information,  
18 Facebook received, stored, and analyzed this information anyway. The report concluded that  
19 "[t]he information provided by Facebook has made it clear that Facebook's internal controls on  
20 this issue have been very limited and were not effective . . . at preventing the receipt of sensitive  
21  
22  
23

---

<sup>82</sup> Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) <https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/>.

1 data.”<sup>83</sup>

2 161. The New York State Department of Financial Service’s concern about Facebook’s  
3 cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a  
4 different settlement involving Facebook’s monetizing of sensitive medical data. In that case, the  
5 more than 100 million users of Flo, a period and ovulation tracking app, learned something  
6 startling: the company was sharing their data with Facebook.<sup>84</sup> When a user was having his period  
7 or informed the app of his intention to get pregnant, Flo would tell Facebook, which could then  
8 use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the  
9 Federal Trade Commission for lying to its users about secretly sharing their data with Facebook,  
10 as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and  
11 Flurry. The FTC reported that Flo “took no action to limit what these companies could do with  
12 users’ information.”<sup>85</sup>

13 162. More recently, Facebook employees admitted to lax protections for sensitive user  
14 data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that  
15 “[w]e do not have an adequate level of control and explainability over how our systems use data,  
16 and thus we can’t confidently make controlled policy changes or external commitments such as  
17 ‘we will not use X data for Y purpose.’”<sup>86</sup>

19 \_\_\_\_\_  
20 <sup>83</sup> New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK  
INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021)

21 [https://www.dfs.ny.gov/system/files/documents/2021/02/facebook\\_report\\_20210218.pdf](https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf).

22 <sup>84</sup> Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.)

23 <https://slate.com/technology/2022/06/health-data-brokers-privacy.html>.

<sup>85</sup> *Id.*

<sup>86</sup> Lorenzo Franceschi-Bicchierai, Facebook Doesn’t Know What It Does with Your Data, or  
Where It Goes: Leaked Document, VICE (April 26, 2022)

<https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes>.

1 163. Furthermore, in June 2022, an investigation by The Markup<sup>87</sup> revealed that the Meta  
2 Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.<sup>88</sup> On those hospital  
3 websites, the Meta Pixel collects and sends Facebook a “packet of data,” including sensitive  
4 personal health information, whenever a user interacts with the website, for example, by clicking  
5 a button to schedule a doctor’s appointment.<sup>89</sup> The data is connected to an IP address, which is “an  
6 identifier that’s like a computer’s mailing address and can generally be linked to a specific  
7 individual or household—creating an intimate receipt of the appointment request for Facebook.”<sup>90</sup>

8 164. During its investigation, The Markup found that Facebook’s purported “filtering”  
9 failed to discard even the most obvious forms of sexual health information. Worse, the article  
10 found that the data that the Meta Pixel was sending Facebook from hospital websites not only  
11 included details such as patients’ medications, descriptions of their allergic reactions, details about  
12 their upcoming doctor’s appointments, but also included patients’ names, addresses, email  
13 addresses, and phone numbers.<sup>91</sup>

14 165. In addition to the 33 hospitals identified by The Markup that had installed the Meta  
15 Pixel on their websites, The Markup identified seven health systems that had installed the Meta  
16 Pixel inside their password-protected patient portals.<sup>92</sup>

17 166. David Holtzman, health privacy consultant and former senior privacy adviser in the  
18

19 \_\_\_\_\_  
20 <sup>87</sup> The Markup is a nonprofit newsroom that investigates how powerful institutions are using  
technology to change our society. See [www.themarkup.org/about](http://www.themarkup.org/about) (last accessed Mar. 19, 2023).

21 <sup>88</sup> Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, Facebook Is Receiving  
Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022 6:00 a.m.)  
22 [https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-](https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites)  
information-from-hospital-websites.

23 <sup>89</sup> *Id.*

<sup>90</sup> *Id.*

<sup>91</sup> *Id.*

<sup>92</sup> *Id.*

1 U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply  
2 troubled" by what the hospitals capturing and sharing patient data in this way.<sup>93</sup>

3 **D. Defendant Violated HIPAA Standards**

4 167. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-  
5 public medical information (PHI) about a patient, a potential patient, or household member of a  
6 patient for marketing purposes without the patients' express written authorization.<sup>94</sup>

7 168. Guidance from the United States Department of Health and Human Services  
8 instructs healthcare providers that patient status alone is protected by HIPAA.

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

12 Identifying information alone, such as personal names, residential addresses, or  
13 phone numbers, would not necessarily be designated as PHI. For instance, if such  
14 information was reported as part of a publicly accessible data source, such as a  
15 phone book, then this information would not be PHI because it is not related to  
16 health data... If such information was listed with health condition, health care  
17 provision, or payment data, such as an indication that the individual was treated at  
18 a certain clinic, then this information would be PHI.<sup>95</sup>

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

17 The HIPAA Privacy Rule gives individuals important controls over whether and  
18 how their protected health information is used and disclosed for marketing  
19 purposes. With limited exceptions, the Rule requires an individual's written  
20 authorization before a use or disclosure of his or his protected health information  
21 can be made for marketing. ... Simply put, a covered entity may not sell protected  
22 health information to a business associate or any other third party for that party's

21 <sup>93</sup> *Id.*

22 <sup>94</sup> HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

23 <sup>95</sup> U.S. Department of Health and Human Services, Guidance Regarding Methods for De-  
identification of Protected Health Information in Accordance with the Health Insurance  
Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012)  
[https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-  
identification/hhs\\_deid\\_guidance.pdf](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf).

1 own purposes. Moreover, covered entities may not sell lists of patients to third  
2 parties without obtaining authorization from each person on the list. (Emphasis  
added).<sup>96</sup>

3 171. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and  
4 Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered  
5 entities and business associates (“regulated entities”) under the HIPAA Privacy, Security, and  
6 Breach Notification Rules (“HIPAA Rules”) when using online tracking technology.<sup>97</sup>

7 172. According to the Bulletin, “HIPAA Rules apply when the information that  
8 regulated entities collect through tracking technologies or disclose to tracking technology vendors  
9 includes protected health information.”<sup>98</sup>

10 173. Citing The Markup’s June 2022 article, the Bulletin expressly notes:

11 Some regulated entities may share sensitive information with online tracking  
12 technology vendors and such sharing may be unauthorized disclosures of PHI with  
13 such vendors. **Regulated entities are not permitted to use tracking technologies  
14 in a manner that would result in impermissible disclosures of PHI to tracking  
15 technology vendors or any other violations of the HIPAA Rules.** For example,  
disclosures of PHI to tracking technology vendors or marketing purposes, without  
16 individuals’ HIPAA-compliant authorizations, would constitute impermissible  
17 disclosures.

18 An impermissible disclosure of an individual’s PHI not only violates the Privacy  
19 Rule but also may result in a wide range of additional harms to the individual or  
20 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

---

21 <sup>96</sup> U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002)  
22 <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/marketing.pdf>.

23 <sup>97</sup> See U.S. Department of Health and Human Services, Use of Online Tracking Technologies by  
HIPAA Covered Entities and Business Associates,  
<https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-online-tracking/index.html>.

<sup>98</sup> *Id.*

1 impermissibly disclose PHI to tracking technology vendors, because of the  
2 proliferation of tracking technologies collecting sensitive information, now more  
3 than ever, it is critical for regulated entities to ensure that they disclose PHI only as  
4 expressly permitted or required by the HIPAA Privacy Rule.<sup>99</sup>

5 174. In other words, HHS has expressly stated that Defendant's conduct of  
6 implementing the Meta Pixel is a violation of HIPAA Rules.

7 **E. Defendant Violated FTC Standards, and the FTC and HHS Take Action**

8 175. The Federal Trade Commission ("FTC") has also recognized that implementation  
9 of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and  
10 "impermissibly disclos[e] consumers' sensitive personal health information to third parties."<sup>100</sup>

11 176. On July 20, 2023, the FTC and HHS sent a "joint letter to approximately 130  
12 hospital systems and telehealth providers to alert them about the risks and concerns about the use  
13 of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online  
14 activities."<sup>101</sup>

15 177. Therein, the FTC reminded healthcare providers that "HIPAA regulated entities are  
16 not permitted to use tracking technologies in a manner that would result in impermissible  
17 disclosures of PHI to third parties or any other violations of the HIPAA Rules"<sup>102</sup> and that "[t]his  
18 is true even if you relied upon a third party to develop your website or mobile app and even if you  
19 do not use the information obtained through use of a tracking technology for any marketing

20 <sup>99</sup> *Id.* (emphasis in original) (internal citations omitted).

21 <sup>100</sup> Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20,  
22 2023) (available at [https://www.ftc.gov/system/files/ftc\\_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf)), **Exhibit A**.

23 <sup>101</sup> FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security  
Risks from Online Tracking Technologies, FEDERAL TRADE COMMISSION (July 20, 2023)  
[https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm\\_source=govdelivery](https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery).

<sup>102</sup> *Id.*

1 purposes.”<sup>103</sup>

2 178. Entities that are not covered by HIPAA also face accountability for disclosing  
3 consumers’ sensitive health information under the Health Breach Notification Rule. 16 C.F.R. §  
4 318. This Rule requires that companies dealing with health records notify the FTC and consumers  
5 if there has been a breach of unsecured identifiable health information, or else face civil penalties  
6 for violations. *Id.* According to the FTC, “a ‘breach’ is not limited to cybersecurity intrusions or  
7 nefarious behavior. Incidents of unauthorized access, *including sharing of covered information*  
8 *without an individual’s authorization*, triggers notification obligations under the Rule.”<sup>104</sup>

9 179. Additionally, the FTC Act makes it unlawful to employ “[u]nfair methods of  
10 competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting  
11 commerce[.]” 15 U.S.C. § 45(a). According to the FTC, “the disclosure of [sensitive health]  
12 information without a consumer’s authorization can, in some circumstances, violate the FTC Act  
13 as well as constitute a breach of security under the FTC’s Health Breach Notification Rule.”<sup>105</sup>

14 180. As such, the FTC and HHS have expressly stated that conduct like Defendant’s  
15 runs afoul of the FTC Act and/or the FTC’s Health Breach Notification Rule.

---

18 <sup>103</sup> *Id.*

19 <sup>104</sup> Statement of the Commission: On Breaches by Health Apps and Other Connected Devices,  
20 U.S. Fed. Trade Commission, (Sept. 15, 2021) (available at  
[https://www.ftc.gov/system/files/documents/public\\_statements/1596364/statement\\_of\\_the\\_commission\\_on\\_breaches\\_by\\_health\\_apps\\_and\\_other\\_connected\\_devices.pdf](https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf)) (emphasis added).

21 <sup>105</sup> *See, e.g.*, U.S. v. Easy Healthcare Corp., Case No. 1:23-cv-3107 (N.D. Ill. 2023),  
<https://www.ftc.gov/legallibrary/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v>; In the Matter of BetterHelp, Inc., FTC Dkt. No. C-4796 (July 14, 2023),  
22 <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter>; U.S.  
23 v. GoodRx Holdings, Inc., Case No. 23-cv-460 (N.D. Cal. 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc>; In the Matter of Flo Health Inc., FTC Dkt. No. C-4747 (June 22, 2021), <https://www.ftc.gov/legal-library/browse/casesproceedings/192-3133-flo-health-inc>.

1       **F. Defendant Violated Industry Standards**

2           181. A medical provider’s duty of confidentiality is a cardinal rule and is embedded in  
3 the physician-patient and hospital-patient relationship.

4           182. The American Medical Association’s (“AMA”) Code of Medical Ethics contains  
5 numerous rules protecting the privacy of patient data and communications, which are applicable  
6 to Banner and its physicians.

7           183. AMA Code of Ethics Opinion 3.1.1 provides:

8           Protecting information gathered in association with the care of the patient is a core  
9 value in health care . . . . Patient privacy encompasses a number of aspects,  
including . . . personal data (informational privacy).

10          184. AMA Code of Medical Ethics Opinion 3.2.4 provides:

11          Information gathered and recorded in association with the care of the patient is  
12 confidential. Patients are entitled to expect that the sensitive personal information  
13 they divulge will be used solely to enable their physician to most effectively provide  
14 needed services. Disclosing information for commercial purposes without consent  
15 undermines trust, violates principles of informed consent and confidentiality, and  
16 may harm the integrity of the patient-physician relationship. Physicians who  
propose to permit third-party access to specific patient information for commercial  
purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully  
inform each patient whose record would be involved (or the patient’s authorized  
surrogate when the individual lacks decision-making capacity about the purposes  
for which access would be granted.

17          185. AMA Code of Medical Ethics Opinion 3.3.2 provides:

18          Information gathered and recorded in association with the care of a patient is  
19 confidential, regardless of the form in which it is collected or stored. Physicians  
20 who collect or store patient information electronically . . . must . . . release patient  
information only in keeping ethics guidelines for confidentiality.

21       **G. Plaintiff’s and Class Members’ Expectation of Privacy**

22           186. At all times when Plaintiff and Class Members provided their Private Information  
23 to Defendant, they all 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



1 marketing and sales purposes, unrelated to patient care.

2 **H. IP Addresses are Personally Identifiable Information**

3 187. Defendant also disclosed and otherwise assisted Facebook and potentially others  
4 with intercepting Plaintiff's and Class Members' IP addresses using the Meta Pixel and other  
5 tracking technologies.

6 188. An IP address is a number that identifies the address of a device connected to the  
7 Internet.

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

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

11 191. Facebook tracks every IP address ever associated with a Facebook user.

12 192. Facebook tracks IP addresses for use of targeting individual homes and their  
13 occupants with advertising.

14 193. Under HIPAA, an IP address is Personally Identifiable Information:

- 15 • HIPAA defines personally identifiable information to include "any unique  
16 identifying number, characteristic or code" and specifically lists the example of IP  
17 addresses. *See* 45 C.F.R. § 164.514 (2).  
18 • HIPAA further declares information as personally identifiable where the covered  
19 entity has "actual knowledge that the information to identify an individual who is a  
20 subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. §  
21 164.514(b)(2)(i)(O).

22 194. Consequently, by disclosing IP addresses, Defendant's business practices violated  
23 HIPAA and industry privacy standards.

1       **I. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized**  
2       **Disclosures**

3           195. The sole purpose for Defendant's use of the Meta Pixel and other tracking  
4       technology was marketing and profits.

5           196. In exchange for disclosing the Private Information of its patients, Defendant is  
6       compensated by Facebook and likely others in the form of enhanced advertising services and more  
7       cost-efficient marketing on its platform.

8           197. Retargeting is a form of online marketing that targets users with ads based on their  
9       previous internet communications and interactions. Upon information and belief, as part of its  
10      marketing campaign, Defendant re-targeted patients and potential patients.

11          198. By utilizing the Meta Pixel and other trackers, the cost of advertising and  
12      retargeting was reduced, thereby benefiting Defendant.

13       **J. Plaintiff's and Class Members' Private Information Had Financial Value**

14          199. The data concerning Plaintiff and Class Members, collected and shared by  
15      Defendant, has tremendous economic value. Data collected via the Meta Pixel, CAPI, and other  
16      online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it  
17      then sells access in the form of targeted advertisements. Targeting works by allowing advertisers  
18      to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook,  
19      are the "people most likely to respond to your ad."<sup>106</sup> Facebook's "Core Audiences" allow  
20      advertisers to target individuals based on demographics, such as age, location, gender, or language,  
21      whereas "Custom Audiences" allow advertisers to target individuals who have "already shown  
22      interest in your business," by visiting a business's website, using an app, or engaging in certain

23      

---

<sup>106</sup> Audience Ad Targeting, Meta, <https://www.facebook.com/business/ads/ad-targeting> (last visited Aug. 14, 2023).

1 online content.<sup>107</sup> Facebook’s “Lookalike Audiences” go further, targeting individuals who  
2 resemble current customer profiles and whom, according to Facebook, “are likely to be interested  
3 in your business.”<sup>108</sup>

4 200. Data harvesting is big business, and it drives Facebook’s profit center, its  
5 advertising sales. In 2019, Facebook generated nearly \$70 billion dollars in advertising revenue  
6 alone, constituting more than 98% of its total revenue for that year.<sup>109</sup>

7 201. This business model is not limited to Facebook. Data harvesting one of the fastest  
8 growing industries in the country, and consumer data is so valuable that it has been described as  
9 the “new oil.” Conservative estimates suggest that in 2018, Internet companies earned \$202 per  
10 American user from mining and selling data. That figure is only due to keep increasing; estimates  
11 for 2022 were as high as \$434 per user, for a total of more than \$200 billion industry wide.

12 202. In particular, the value of health data is well-known due to the media’s extensive  
13 reporting on the subject. For example, Time Magazine published an article in 2017 titled “How  
14 Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry.” Therein, Time Magazine  
15 described the extensive market for health data and observed that the health data market is both  
16 lucrative and a significant risk to privacy.<sup>110</sup>

17 203. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-  
18 identified patient data has become its own small economy: There’s a whole market of brokers who  
19

---

20 <sup>107</sup> *Id.*

21 <sup>108</sup> See How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Center,  
<https://www.facebook.com/business/help/465262276878947> (last visited Aug. 14, 2023).

22 <sup>109</sup> See Here’s How Big Facebook’s Ad Business Really Is, CNN,  
<https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html> (last visited  
23 Aug. 14, 2023).

<sup>110</sup> See Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry,  
TIME, (Jan. 9, 2017 at 9:00 a.m.) <https://time.com/4588104/medical-data-industry/>.

1 compile the data from providers and other health-care organizations and sell it to buyers.”<sup>111</sup>

2 **TOLLING, CONCEALMENT, AND ESTOPPEL**

3 204. The applicable statutes of limitation have been tolled as a result of Banner’s  
4 knowing and active concealment and denial of the facts alleged herein.

5 205. Banner seamlessly incorporated Meta Pixel and other trackers into its Website and  
6 Online Platforms while providing users with no indication that their Website usage was being  
7 tracked and transmitted to third parties. Banner knew that its Website incorporated Meta Pixel and  
8 other trackers, yet it failed to disclose to Plaintiff and Class Members that their sensitive medical  
9 information would be intercepted, collected, used by, and disclosed to Facebook and likely other  
10 third parties.

11 206. Plaintiff and Class Members could not with due diligence have discovered the full  
12 scope of Banner’s conduct, because there were no disclosures or other indication that they were  
13 interacting with websites employing Meta Pixel or any other tracking technology.

14 207. All applicable statutes of limitation have also been tolled by operation of the  
15 discovery rule and the doctrine of continuing tort. Banner’s illegal interception and disclosure of  
16 Plaintiff’s Private Information has continued unabated. What is more, Banner was under a duty to  
17 disclose the nature and significance of its data collection practices but did not do so. Banner is  
18 therefore estopped from relying on any statute of limitations defenses.

19  
20  
21  
22  
23 <sup>111</sup> See Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) <https://www.cnbc.com/2019/12/18/hospital-exec-say-theyre-flooded-with-requests-for-your-health-data.html>.

1 **CLASS ALLEGATIONS**

2 208. Plaintiff brings this nationwide class action individually, and on behalf of all other  
3 similarly situated persons, pursuant to Cal. Civ. P. § 382.

4 209. The nationwide Class that Plaintiff seeks to represent is defined as follows:

5 **All persons whose Private Information was disclosed by Defendant to third**  
6 **parties through the Meta Pixel and related technology without authorization.**

7 210. Excluded from the Class are the following individuals and/or entities: Defendant  
8 and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which  
9 Defendant has a controlling interest; all individuals who make a timely election to be excluded  
10 from this proceeding using the correct protocol for opting out; any and all federal, state, or local  
11 governments, including but not limited to their departments, agencies, divisions, bureaus, boards,  
12 sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this  
13 litigation, as well as their immediate family members.

14 211. Plaintiff reserves the right to modify or amend the definition of the proposed class  
15 before the Court determines whether certification is appropriate.

16 212. Numerosity: Class Members are so numerous that joinder of all members is  
17 impracticable. Upon information and belief, there are hundreds or thousands of individuals whose  
18 Private Information may have been improperly used or disclosed by Defendant, and the Class is  
19 identifiable within Defendant's records.

20 213. Commonality: Questions of law and fact common to the Class exist and  
21 predominate over any questions affecting only individual Class Members. These include:

- 22 a. whether and to what extent Defendant had a duty to protect Plaintiff's and  
23 Class Members' Private Information;
- b. whether Defendant had duties not to disclose the Plaintiff's and Class

- 1 Members' Private Information to unauthorized third parties;
- 2 c. whether Defendant had duties not to use Plaintiff's and Class Members'
- 3 Private Information for non-healthcare purposes;
- 4 d. whether Defendant had duties not to use Plaintiff's and Class Members'
- 5 Private Information for unauthorized purposes;
- 6 e. whether Defendant failed to adequately Plaintiff's and Class Members'
- 7 Private Information;
- 8 f. whether Defendant adequately, promptly, and accurately informed Plaintiff
- 9 and Class Members that their Private Information had been compromised;
- 10 g. whether Defendant violated the law by failing to promptly notify Plaintiff
- 11 and Class Members that their Private Information had been compromised;
- 12 h. whether Defendant failed to properly implement and configure the tracking
- 13 software on its Online Platforms to prevent the disclosure of confidential
- 14 communications and Private Information;
- 15 i. whether Defendant committed invasion of privacy;
- 16 j. whether Defendant breached its implied contracts with Plaintiff and the
- 17 Class Members;
- 18 k. or in the alternate, whether Defendant was unjustly enriched;
- 19 l. whether Defendant breached fiduciary duties to Plaintiff and the Class
- 20 Members;
- 21 m. whether Defendant violated the California Invasion of Privacy Act
- 22 ("CIPA"), Cal. Penal Code §§ 630, *et seq.*;
- 23 n. whether Defendant violated the California Confidentiality of Medical

1 Information Act (“CMIA”), Cal. Civil Code §§ 56.06, 56.10, and 56.101;

2 o. whether Defendant violated the Comprehensive Computer Data Access and  
3 Fraud Act (“CDAFA”), Cal. Penal Code § 502;

4 p. whether Defendant engaged in unfair, unlawful, or deceptive practices in  
5 violation of Cal. Bus. & Prof. Code §§ 17200, *et. seq.*; and,

6 q. whether Plaintiff and the Class Members are entitled to monetary damages,  
7 including compensatory and statutory damages, and the sums thereof.

8 214. Typicality: Plaintiff’s claims are typical of those of other Class Members because  
9 all had their Private Information compromised as a result of Defendant’s use and incorporation of  
10 Meta Pixel and other tracking technology.

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

18 216. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of  
19 the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic  
20 to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the  
21 Class Members and the infringement of the rights and the damages Plaintiff has suffered is typical  
22 of other Class Members. Plaintiff has also retained counsel experienced in complex class action  
23 litigation, and Plaintiff intends to prosecute this action vigorously.

1           217. Superiority and Manageability: Class litigation is an appropriate method for fair  
2 and efficient adjudication of the claims involved. Class action treatment is superior to all other  
3 available methods for the fair and efficient adjudication of the controversy alleged herein; it will  
4 permit a large number of Class Members to prosecute their common claims in a single forum  
5 simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and  
6 expense that hundreds of individual actions would require. Class action treatment will permit the  
7 adjudication of relatively modest claims by certain Class Members, who could not individually  
8 afford to litigate a complex claim against large corporations, like Defendant. Further, even for  
9 those Class Members who could afford to litigate such a claim, it would still be economically  
10 impractical and impose a burden on the courts.

11           218. The nature of this action and the nature of laws available to Plaintiff and Class  
12 Members make the use of the class action device a particularly efficient and appropriate procedure  
13 to afford relief to Plaintiff and Class Members for the wrongs alleged. If the class action device  
14 were not used, Defendant would necessarily gain an unconscionable advantage because they would  
15 be able to exploit and overwhelm the limited resources of each individual Class Member with  
16 superior financial and legal resources. Moreover, the costs of individual suits could unreasonably  
17 consume the amounts that would be recovered, whereas proof of a common course of conduct to  
18 which Plaintiff were exposed is representative of that experienced by the Class and will establish  
19 the right of each Class Member to recover on the cause of action alleged. Finally, individual actions  
20 would create a risk of inconsistent results and would be unnecessary and duplicative of this  
21 litigation.

22           219. The litigation of the claims brought herein is manageable. Defendant's uniform  
23 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class



1 Members demonstrates that there would be no significant manageability problems with  
2 prosecuting this lawsuit as a class action.

3 220. Adequate notice can be given to Class Members directly using information  
4 maintained in Defendant's records.

5 221. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful  
6 use and disclosure and failure to properly secure the Private Information of Class Members,  
7 Defendant may continue to refuse to provide proper notification to and obtain proper consent from  
8 Class Member, and Defendant may continue to act unlawfully as set forth in this Complaint.

9 222. Further, Defendant has acted or refused to act on grounds generally applicable to  
10 the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the  
11 whole of the Class is appropriate.

12 223. Likewise, particular issues are appropriate for certification because such claims  
13 present only particular, common issues, the resolution of which would advance the disposition of  
14 this matter and the parties' interests therein. Such particular issues include, but are not limited to  
15 the following:

- 16 a. whether Defendant owed a legal duty to Plaintiff and Class Members to  
17 exercise due care in collecting, storing, using, and safeguarding their Private  
18 Information;
- 19 b. whether Defendant breached a legal duty to Plaintiff and Class Members to  
20 exercise due care in collecting, storing, using, and safeguarding their Private  
21 Information;
- 22 c. whether Defendant failed to comply with its own policies and applicable  
23 laws, regulations, and industry standards relating to the disclosure of patient

- 1 information;
- 2 d. whether an implied contract existed between Defendant on the one hand,
- 3 and Plaintiff and Class Members on the other, and the terms of that implied
- 4 contract;
- 5 e. whether Defendant breached the implied contract;
- 6 f. in the alternate, whether Defendant was unjustly enriched;
- 7 g. whether Defendant adequately and accurately informed Plaintiff and Class
- 8 Members that their Private Information had been used and disclosed to third
- 9 parties;
- 10 h. whether Defendant failed to implement and maintain reasonable security
- 11 procedures and practices;
- 12 i. whether Defendant committed an invasion of privacy;
- 13 j. whether Defendant had fiduciary duties to Plaintiff and the Class Members;
- 14 k. whether Defendant breached its fiduciary duties;
- 15 l. whether Defendant violated the California Invasion of Privacy Act
- 16 (“CIPA”), Cal. Penal Code §§ 630, *et seq.*;
- 17 m. whether Defendant violated the California Confidentiality of Medical
- 18 Information Act (“CMIA”), Cal. Civil Code §§ 56.06, 56.10, and 56.101;
- 19 n. whether Defendant violated the Comprehensive Computer Data Access and
- 20 Fraud Act (“CDAFA”), Cal. Penal Code § 502;
- 21 o. whether Defendant engaged in unfair, unlawful, or deceptive practices in
- 22 violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*; and,
- 23 p. whether Plaintiff and the Class Members are entitled to actual,

1 consequential, and/or nominal damages, and/or injunctive relief as a result  
2 of Defendant's wrongful conduct.

3 **COUNT I**  
4 **NEGLIGENCE**  
5 **(On Behalf of Plaintiff and the Class)**

6 224. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

7 225. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care  
8 in handling and using Plaintiff's and Class Members' Private Information in its care and custody,  
9 including implementing industry-standard privacy procedures sufficient to reasonably protect the  
10 information from the disclosure and unauthorized transmittal and use of Private Information that  
11 occurred.

12 226. Defendant acted with wanton and reckless disregard for the privacy and  
13 confidentiality of Plaintiff's and Class Members' Private Information by disclosing and providing  
14 access to this information to third parties for the financial benefit of the third parties and Defendant.

15 227. Defendant owed these duties to Plaintiff and Class Members because they are  
16 members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew  
17 or should have known would suffer injury-in-fact from Defendant's Disclosure of their Private  
18 Information to benefit third parties and Defendant. Defendant actively sought and obtained  
19 Plaintiff's and Class Members' Private Information.

20 228. Private Information is highly valuable, and Defendant knew, or should have known,  
21 the harm that would be inflicted on Plaintiff and Class Members by disclosing their Private  
22 Information to third parties. This disclosure was of benefit to third parties and Defendant by way  
23 of data harvesting, advertising, and increased sales.

24 229. Defendant breached its common law duties by failing to exercise reasonable care

1 in the handling and securing of Private Information of Plaintiff and Class Members and in the  
2 supervising its agents, contractors, vendors, and suppliers in the handling and securing of Private  
3 Information of Plaintiff and Class Members. This failure actually and proximately caused  
4 Plaintiff's and Class Members' injuries.

5 230. In addition, the standards of care owed by Defendant are established by statute,  
6 including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160  
7 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health  
8 Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected  
9 Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections  
10 identified above, under which Defendant were required by law to maintain adequate and  
11 reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and  
12 Class Members' Private Information.

13 231. Plaintiff and Class Members are within the class of persons that these statutes and  
14 rules were designed to protect.

15 232. Defendant had a duty to have procedures in place to detect and prevent the loss or  
16 unauthorized dissemination of Plaintiff's and Class Members' Private Information, PII and PHI.

17 233. Defendant owed a duty to timely and adequately inform Plaintiff and Class  
18 Members, in the event of their Private Information, PII and PHI, being improperly disclosed to  
19 unauthorized third parties.

20 234. It was not only reasonably foreseeable, but it was intended, that the failure to  
21 reasonably protect and secure Plaintiff's and Class Members' Private Information, PII and PHI, in  
22 compliance with applicable laws would result in an unauthorized third-parties such as Facebook,  
23 and others gaining access to Plaintiff's and Class Members' PII and PHI, and resulting in

1 Defendant's liability under principles of negligence and negligence *per se*.

2 235. Defendant violated the standards of care under Section 5 of the FTC Act and under  
3 HIPAA and attendant regulations by failing to use reasonable measures to protect Plaintiff's and  
4 Class Members' PII and PHI and not complying with applicable industry standards as described  
5 in detail herein.

6 236. As a direct and traceable result of Defendant's negligence and/or negligent  
7 supervision, and/or negligence *per se*, Plaintiff and Class Members have suffered or will suffer  
8 damages, including monetary damages, inappropriate advertisements, and use of their Private  
9 Information for advertising purposes, and increased risk of future harm, embarrassment,  
10 humiliation, frustration, and emotional distress.

11 237. Plaintiff's and Class Member's PII and PHI constitute personal property that was  
12 taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury, and  
13 damages to Plaintiff and Class Members.

14 238. Defendant's breach of its common-law duties to exercise reasonable care and  
15 negligence directly and proximately caused Plaintiff's and Class Members' actual, tangible, injury-  
16 in-fact and damages, including, without limitation, the unauthorized access of their Private  
17 Information by third parties, improper disclosure of their Private Information, lost benefit of their  
18 bargain, lost value of their Private Information and diminution in value, emotional distress, and  
19 lost time and money incurred to mitigate and remediate the effects of use of their information that  
20 resulted from and were caused by Defendant's negligence. These injuries are ongoing, imminent,  
21 immediate, and continuing.

22 239. In failing to secure Plaintiff's and Class Members' Private Information, PII and  
23 PHI, Defendant are guilty of oppression, fraud, or malice. Defendant acted or failed to act with a

1 reckless, willful, or conscious disregard of Plaintiff and Class Members' rights. Plaintiff, in  
2 addition to seeking actual damages, also seek punitive damages on behalf of themselves and the  
3 Class.

4 240. Defendant's negligence directly and proximately caused the unauthorized access  
5 and Disclosure of Plaintiff's and Class Members' Private Information, PII and PHI, and as a result,  
6 Plaintiff and Class Members have suffered and will continue to suffer damages as a result of  
7 Defendant's conduct. Plaintiff and Class Members seek actual, compensatory, and punitive  
8 damages, and all other relief they may be entitled to as a proximate result of Defendant's  
9 negligence and negligence *per se*.

10 **COUNT II**  
11 **BREACH OF IMPLIED CONTRACT**  
12 **(On behalf of Plaintiff and the Class)**

13 241. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

14 242. As a condition of receiving medical care from Defendant, Plaintiff and the Class  
15 provided their Private Information and paid monies for medical treatment received. In so doing,  
16 Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant  
17 agreed to safeguard and protect such information, as set forth in its Privacy Policies, and elsewhere,  
18 to keep such information secure and confidential.

19 243. Implicit in the agreement between Defendant and its patients, Plaintiff and the  
20 proposed Class Members, was the obligation that all parties would maintain the Private  
21 Information confidentially and securely.

22 244. Defendant had an implied duty of good faith to ensure that the Private Information  
23 of Plaintiff and Class Members in its possession was only used only as authorized, such as to  
provide medical treatment, billing, and other medical benefits from Defendant.

1           245. Defendant had an implied duty to protect the Private Information of Plaintiff and  
2 Class Members from unauthorized disclosure or uses.

3           246. Additionally, Defendant explicitly promised to keep its patients' Private  
4 Information secure and confidential, stating in its Notice of Privacy Practices that, “[o]ther uses  
5 and disclosures not described in this notice will be made only with your written  
6 authorization, such as sale of medical information..”<sup>112</sup>

7           247. Plaintiff and Class Members fully performed their obligations under the implied  
8 contracts with Defendant, but Banner did not. Plaintiff and Class Members would not have  
9 provided their confidential Private Information to Defendant in the absence of their implied  
10 contracts with Defendant that their Private Information would be kept in confidence and would  
11 instead have retained the opportunity to control their Private Information for uses other than  
12 receiving medical treatment from Defendant.

13           248. Defendant breached the implied contracts with Plaintiff and Class members by  
14 disclosing Plaintiff's and Class Members' Private Information to unauthorized third parties.

15           249. Defendant's acts and omissions have materially affected the intended purpose of  
16 the implied contracts that required Plaintiff and Class Members to provide their Private  
17 Information in exchange for medical treatment and benefits.

18           250. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff  
19 and the Class have suffered (and will continue to suffer) actual, tangible, injury-in-fact and  
20 damages, including, without limitation, the unauthorized access of their Private Information by  
21 third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost  
22 value of their Private Information and diminution in value, emotional distress, and lost time and  
23

---

<sup>112</sup> *Notice of Privacy Practices, Exhibit B* (bold emphasis added).

1 money incurred to mitigate and remediate the effects of use of their information that resulted from  
2 and were caused by Defendant's breach of implied contract. These injuries are ongoing, imminent,  
3 immediate, and continuing.

4 251. As a direct and proximate result of Defendant's above-described breach of contract,  
5 Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

6 **COUNT III**  
7 **UNJUST ENRICHMENT**  
8 **(On Behalf of Plaintiff and the Class)**

9 252. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

10 253. This claim is pleaded solely in the alternative to Plaintiff's breach of implied  
11 contract claim.

12 254. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the  
13 form of valuable sensitive medical information that Defendant collected from Plaintiff and Class  
14 Members under the guise of keeping this information private. Defendant collected, used, and  
15 disclosed this information for their own gain, for marketing purposes, and for sale or trade with  
16 third parties.

17 255. Plaintiff and Class Members would not have used Defendant's services or would  
18 have paid less for those services, if they had known that Defendant would collect, use, and disclose  
19 their Private Information to third parties.

20 256. Defendant appreciated or had knowledge of the benefits conferred upon them by  
21 Plaintiff and Class Members.

22 257. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual  
23 damages in an amount equal to the difference in value between their purchases made with  
reasonable data privacy practices and procedures that Plaintiff and Class Members paid for, and



1 those purchases without unreasonable data privacy practices and procedures that they received.

2 258. The benefits that Defendant derived from Plaintiff and Class Members rightly  
3 belong to Plaintiff and Class Members themselves. Under unjust enrichment principles, it would  
4 be inequitable for Defendant to retain the profit and/or other benefits it derived from the unfair and  
5 unconscionable methods, acts, and trade practices alleged in this Complaint.

6 259. Defendant should be compelled to disgorge into a common fund for the benefit of  
7 Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of its  
8 conduct and the unauthorized Disclosure alleged herein.

9 **COUNT IV**  
10 **BREACH OF FIDUCIARY DUTY**  
**(On Behalf of Plaintiff and the Class)**

11 260. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

12 261. A relationship existed between Plaintiff and the Class, on the one hand, and  
13 Defendant, on the other, in which Plaintiff and the Class put their trust in Defendant to protect the  
14 Private Information of Plaintiff and the Class, and Defendant accepted that trust.

15 262. Defendant breached the fiduciary duty that it owed to Plaintiff and the Class  
16 Members by failing to act with the utmost good faith, fairness, and honesty; failing to act with the  
17 highest and finest loyalty; and failing to protect and, indeed, intentionally disclosing, their Private  
18 Information.

19 263. Defendant's breach of fiduciary duty was a legal cause of injury-in-fact and  
20 damages to Plaintiff and the Class.

21 264. But for Defendant's breach of fiduciary duty, the injury-in-fact and damages to  
22 Plaintiff and the Class would not have occurred.

23 265. Defendant's breach of fiduciary duty substantially contributed to the injury and

1 damages to the Plaintiff and the Class.

2 266. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff  
3 and Class Members are entitled to and demand actual, consequential, and nominal damages,  
4 injunctive relief, and all other relief allowed by law.

5 **COUNT V**  
6 **INVASION OF PRIVACY—INTRUSION UPON SECLUSION**  
7 **(On Behalf of Plaintiff and the Class)**

8 267. Plaintiff re-allege and incorporate the above allegations as if fully set forth herein.

9 268. Plaintiff and Class Members had a reasonable expectation of privacy in their  
10 communications with Defendant via its Websites and Online Platforms.

11 269. Plaintiff and Class Members communicated sensitive PHI and PII—Private  
12 Information—that they intended for only Defendant to receive and that they understood Defendant  
13 would keep private.

14 270. Defendant's disclosure of the substance and nature of those communications to  
15 third parties without the knowledge and consent of Plaintiff and Class Members is an intentional  
16 intrusion on Plaintiff's and Class Members' solitude or seclusion in their private affairs and  
17 concerns.

18 271. Plaintiff and Class Members had a reasonable expectation of privacy given  
19 Defendant's representations in its Privacy Policies, and elsewhere. Moreover, Plaintiff and Class  
20 Members have a general expectation that their communications regarding healthcare with their  
21 healthcare providers will be kept confidential. Defendant's disclosure of PHI coupled with PII is  
22 highly offensive to the reasonable person.

23 272. As a result of Defendant's tortious conduct, Plaintiff and Class Members have  
suffered harm and injury, including but not limited to an invasion of their privacy rights.



1 intrusion on Plaintiff's and Class Members' solitude or seclusion in their private affairs and  
2 concerns.

3 282. Plaintiff and Class Members had a reasonable expectation of privacy given  
4 Defendant's representations in their Privacy Policies, and elsewhere. Moreover, Plaintiff and Class  
5 Members have a general expectation that their communications regarding healthcare with their  
6 healthcare providers will be kept confidential. Defendant's disclosure of PHI coupled with PII is  
7 highly offensive to the reasonable person.

8 283. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm  
9 and injury, including but not limited to an invasion of their privacy rights under the California  
10 Constitution.

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

14 285. Plaintiff and Class Members seek appropriate relief for that injury, including but  
15 not limited to, damages that will reasonably compensate Plaintiff and Class Members for the harm  
16 to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

17 286. Plaintiff and Class Members are also entitled to punitive damages resulting from  
18 the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff  
19 and Class Members in conscious disregard of their rights. Such damages are needed to deter  
20 Defendant from engaging in such conduct in the future.

21 287. Plaintiff also seek such other relief as the Court may deem just and proper.  
22  
23

1 **COUNT VII**  
2 **VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (“CIPA”),**  
3 **CAL. PENAL CODE §§ 630, *ET SEQ.***  
4 **(On Behalf of Plaintiff and the Class)**

5 288. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

6 289. The California Legislature enacted the California Invasion of Privacy Act, Cal.  
7 Penal Code §§ 630, *et seq.* (“CIPA”) declaring that:

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

13 The Legislature by this chapter intends to protect the right of privacy of the people  
14 of this state.

15 Cal. Penal Code §§ 630.

16 290. Cal. Penal Code § 631(a) prohibits persons from “aid[ing], agree[ing] with,  
17 employ[ing], or conspir[ing] with” a third party to “read[], or attempt[] to read, or to learn the  
18 contents or meaning of any message, report, or communication while the same is in transit or  
19 passing over any wire, line, or cable, or is being sent from, or received at any place within this  
20 state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any  
21 way, any information so obtained” “by means of any machine, instrument, or contrivance, or in  
22 any other manner...” Cal. Penal Code § 631(a).

23 291. Cal. Penal Code § 632(a) prohibits persons from intentionally recording  
confidential communications without consent of all parties to the communication.

292. All alleged communications between Plaintiff or Class Members and Defendant  
qualify as protected communications under CIPA because each communication is made using  
personal computing devices (e.g., computers, smartphones, tablets) that send and receive

1 communications in whole or in part through the use of facilities used for the transmission of  
2 communications aided by wire, cable, or other like connections.

3 293. As alleged in the preceding paragraphs, by use of the Meta Pixel and other tracking  
4 technologies, Defendant used a recording device to record the confidential communications  
5 without the consent of Plaintiff or Class members and then transmitted such information to others,  
6 such as Facebook.

7 294. At all relevant times, Defendant's aiding of Facebook, and other third parties to  
8 learn the contents of communications and Defendant's recording of confidential communications  
9 was without Plaintiff's and the Class Members' authorization and consent.

10 295. Plaintiff and Class Members had a reasonable expectation of privacy regarding the  
11 confidentiality of their communications with Defendant. Defendant promised them that it would  
12 safeguard their personal information, and that "[o]ther uses and disclosures not described in this  
13 notice will be made only with your written authorization, such as sale of medical information..."<sup>113</sup>  
14 Defendant never received any authorization and disclosed Plaintiff's and the Class's Private  
15 Information anyways.

16 296. Defendant engaged in and continued to engage in interception by aiding others  
17 (including Facebook) to secretly record the contents of Plaintiff's and Class Members' wire  
18 communications.

19 297. The intercepting devices used in this case include, but are not limited to:

- 20 a. those to which Plaintiff's and Class Members' communications were  
21 disclosed;
- 22 b. Plaintiff's and Class Members' personal computing devices;
- 23

---

<sup>113</sup> *Notice of Privacy Practices, Exhibit B.*

- 1 c. Plaintiff's and Class Members' web browsers;
- 2 d. Plaintiff's and Class Members' browser-managed files;
- 3 e. the Meta Pixel;
- 4 f. internet cookies;
- 5 g. other pixels, trackers, and/or tracking technology installed on Defendant's
- 6 Website and/or server;
- 7 h. Defendant's computer servers;
- 8 i. third-party source code utilized by Defendant; and
- 9 j. computer servers of third parties (including Facebook).

10 298. Defendant aided in the interception of contents in that the data from the  
11 communications between Plaintiff and/or Class Members and Defendant that were redirected to  
12 and recorded by the third parties, including Facebook, include information which identifies the  
13 parties to each communication, their existence, and their contents.

14 299. Plaintiff and Class Members reasonably expected that their Private Information was  
15 not being intercepted, recorded, and disclosed to Facebook, and other third parties.

16 300. No legitimate purpose was served by Defendant's willful and intentional disclosure  
17 of Plaintiff's and Class Members' Private Information to Facebook, and other third parties. Neither  
18 Plaintiff nor Class Members consented to the disclosure of their Private Information by Defendant  
19 to Facebook, and other third parties.

20 301. The tracking pixels that Defendant utilized are designed such that they transmitted  
21 each of a website user's actions to third parties alongside and contemporaneously with the user  
22 initiating the communication. Thus, Plaintiff and Class Members' communications were  
23 intercepted in transit to the intended recipient (Defendant) before they reached Defendant's

1 servers.

2 302. Defendant willingly facilitated Facebook's interception and collection of Plaintiff's  
3 and Class Members' Private Information by embedding pixels on its Online Platforms. Moreover,  
4 Defendant had full control over these tracking pixels, including which webpages contained the  
5 pixels, what information was tracked and shared, and how events were categorized prior to  
6 transmission.

7 303. Defendant gave substantial assistance to Facebook in violating the privacy rights  
8 of its patients, despite the fact that Defendant's conduct constituted a breach of the duties of  
9 confidentiality that medical providers owe their patients. Defendant knew that the installation of  
10 the Meta Pixel on its website would result in the unauthorized disclosure of its patients'  
11 communications to Facebook, yet nevertheless did so anyway.

12 304. Plaintiff's and Class Members' electronic communications were intercepted during  
13 transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their  
14 Private Information, including using their sensitive medical information to develop marketing and  
15 advertising strategies. The private information that Defendant assisted Facebook, and other third  
16 parties with reading, learning, and exploiting, including Plaintiff's and Class Member's medical  
17 conditions, their medical concerns, and their past, present, and future medical treatment.

18 305. Plaintiff and the Class Members seek statutory damages under Cal. Penal Code §  
19 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount  
20 of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as  
21 injunctive or other equitable relief.

22 306. In addition to statutory damages, Defendant's violations caused Plaintiff and Class  
23 Members the following damages.



- 1 a. Sensitive and confidential information that Plaintiff and Class Members  
2 intended to remain private is no longer private.
- 3 b. Defendant eroded the essential confidential nature of the doctor-patient  
4 relationship.
- 5 c. Defendant took something of value from Plaintiff and Class Members and  
6 derived benefit therefrom without Plaintiff's and Class Members'  
7 knowledge or informed consent and without sharing the benefit of such  
8 value;
- 9 d. Plaintiff and Class Members did not get the full value of the medical  
10 services for which they paid, which included Defendant's duty to maintain  
11 confidentiality; and
- 12 e. Defendant's actions diminished the value of Plaintiff's and Class Members'  
13 personal information.

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

16 **COUNT VIII**  
17 **VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL**  
18 **INFORMATION ACT ("CMIA"), CAL. CIVIL CODE §§ 56.06, 56.10, 56.101**  
19 **(On behalf of Plaintiff and the Class)**

20 308. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

21 Civil Code § 56.06

22 309. Defendant is a provider of health care under Cal. Civil Code. § 56.06, subdivisions  
23 (a) and (b), because it maintains medical information and offers software to consumers that is  
designed to maintain medical information for the purposes of allowing their users to manage their  
information or for the diagnosis, treatment, or management of a medical condition.

1           310. Defendant is therefore subject to the requirements of the CMIA and obligated under  
2 Cal. Civil Code. § 56.06(d) to maintain the same standards of confidentiality required of a provider  
3 of health care with respect to medical information disclosed to it.

4           311. By conduct complained of in the preceding paragraphs, Defendant violated Cal.  
5 Civil Code § 56.06 by failing to maintain the confidentiality of users' medical information, Private  
6 Information, and instead, disclosing Plaintiff's and Class Members' medical information/Private  
7 Information to Facebook and likely other third parties without consent. This information was  
8 intentionally shared with Facebook and others, whose business is to sell advertisements based on  
9 the data that they collect about individuals, including the data Plaintiff and the Class Members  
10 shared with Defendant.

11           312. As set forth above, Defendant knowingly shared information such as identities,  
12 device identifiers, IP addresses, web URLs, possibly Facebook IDs, and other data that could be  
13 used to identify Plaintiff and Class Members in combination with their health information, such as  
14 searches and appointments. This information constitutes confidential information under the CMIA.

15           313. Defendant knowingly and willfully, or negligently, disclosed medical information  
16 of Plaintiff and the proposed Class, without consent, to Facebook for financial gain. Defendant's  
17 acts were knowing and willful as Defendant were aware that Facebook would collect all data  
18 inputted while using their websites, yet intentionally embedded Meta Pixel anyway.

19           314. Defendant's decisions to affirmatively share and communicate its patients'  
20 PHI/Private Information with Facebook resulted in one or more unauthorized persons improperly  
21 accessing and reviewing Plaintiff's and the Class Members' PHI.

22  
23

1 Cal. Civil Code § 56.10(a)

2 315. Cal. Civil Code § 56.10(a) prohibits a health care provider from disclosing medical  
3 information without first obtaining an authorization, unless a statutory exception applies.

4 316. By conduct complained of in the preceding paragraphs, Defendant disclosed  
5 medical information, Private Information, of Plaintiff and the Class Members without first  
6 obtaining authorization when it disclosed their sensitive medical information to Facebook, and  
7 other third parties without consent, including PHI and PII. No statutory exception applies.

8 317. As a result, Defendant violated Cal. Civil Code § 56.10(a).

9 Cal. Civil Code § 56.101(a)

10 318. Cal. Civil Code § 56.101(a) requires that every provider of health care “who  
11 creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall  
12 do so in a manner that preserves the confidentiality of the information contained therein.”

13 319. Any health care provider who “negligently creates, maintains, preservers, stores,  
14 abandons, destroys, or disposes of medical information shall be subject to the remedies and  
15 penalties provided under subdivisions (b) and (c) of Section 56.36.”

16 320. By conduct complained of in the preceding paragraphs, Defendant failed to  
17 maintain, preserve, and store medical information/Private Information of Plaintiff and the Class  
18 Members in a manner that preserves the confidentiality of the information contained therein by  
19 disclosing their PHI/Private Information to Facebook, and other third parties without consent.

20 321. Defendant’s failures to maintain, preserve, and store medical information in a  
21 manner that preserves the confidentiality of the information was, at the least, negligent and violates  
22 Cal. Civil Code § 56.36(b) and (c).

23

1           322. Accordingly, as a result of Defendant's violations of Cal. Civil Code §§ 56.06,  
2 56.10, and Cal. Civil Code 56.101, Plaintiff and Class Members are entitled to: (1) nominal  
3 damages of \$1,000; (2) actual damages, in an amount to be determined at trial; (3) statutory  
4 damages pursuant to 56.36(c); and (4) reasonable attorney's fees and other litigation costs  
5 reasonably incurred.

6           323. In addition to statutory damages, Defendant's breach of Cal. Civil Code §§ 56.06,  
7 56.10, and 56.101, caused Plaintiff and Class Members, at minimum, the following damages:

- 8           a. Sensitive and confidential information that Plaintiff and Class Members  
9 intended to remain private is no longer private.
- 10           b. Defendant eroded the essential confidential nature of the doctor-patient  
11 relationship.
- 12           c. Defendant took something of value from Plaintiff and Class Members and  
13 derived benefit therefrom without Plaintiff's and Class Members'  
14 knowledge or informed consent and without sharing the benefit of such  
15 value;
- 16           d. Plaintiff and Class Members did not get the full value of the medical  
17 services for which they paid, which included Defendant's duty to maintain  
18 confidentiality; and
- 19           e. Defendant's actions diminished the value of Plaintiff's and Class Members'  
20 personal information.

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

23

1 **COUNT IX**  
2 **VIOLATION OF THE COMPREHENSIVE COMPUTER DATA ACCESS**  
3 **AND FRAUD ACT (“CDAFA”), CAL. PENAL CODE § 502.**  
4 **(On Behalf of Plaintiff and the Class)**

5 325. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

6 326. The California Legislature enacted the Comprehensive Computer Data Access and  
7 Fraud Act, CAL. PENAL CODE § 502 (“CDAFA”) to “expand the degree of protection afforded to  
8 individuals, businesses, and governmental agencies from tampering, interference, damage, and  
9 unauthorized access to lawfully created computer data and computer systems,” and finding and  
10 declaring “that the proliferation of computer technology has resulted in a concomitant proliferation  
11 of computer crime and other forms of unauthorized access to computers, computer systems, and  
12 computer data.” Cal. Penal Code § 502(a).

13 327. In enacting the CDAFA, the Legislature further found and declared “that protection  
14 of the integrity of all types and forms of lawfully created computers, computer systems, and  
15 computer data is vital to the protection of the privacy of individuals as well as to the well-being of  
16 financial institutions, business concerns, governmental agencies, and others within this state that  
17 lawfully utilize those computers, computer systems, and data.” Cal. Penal Code § 502(a).

18 328. Plaintiff’s and the Class Members’ devices on which they accessed Defendant’s  
19 Online Platforms and Websites, including their computers, smart phones, and tablets, constitute  
20 computers or “computer systems” within the meaning of CDAFA. Cal. Penal Code § 502(b)(5).

21 329. By conduct complained of in the preceding paragraphs, Defendant violated Section  
22 502(c)(1)(B) of CDAFA by knowingly accessing without permission Plaintiff’s and Class  
23 Members’ devices in order to wrongfully obtain and use their personal data, including their  
sensitive medical information, all Private Information, in violation of Plaintiff’s and Class  
Members’ reasonable expectations of privacy in their devices and data.

1           330. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly and without  
2 permission accessing, taking, copying, and using Plaintiff's and the Class Members' Private  
3 Information, PHI and PII, including their sensitive medical information.

4           331. Defendant used Plaintiff's and Class Members' data as part of a scheme to defraud  
5 them and wrongfully obtain their data and other economic benefits. Specifically, Defendant  
6 intentionally concealed from Plaintiff and Class Members that Defendant had secretly installed  
7 tracking pixels on its Online Platforms that surreptitiously shared patient data with third party  
8 advertising companies like Facebook. Had Plaintiff and Class Members been aware of this  
9 practice, they would not have used Defendant's Website and Online Platforms.

10           332. The computers and mobile devices that Plaintiff and Class Members used when  
11 accessing Defendant's Online Platforms all have and operate "computer services" within the  
12 meaning of CDAFA. Defendant violated §§ 502(c)(3) and (7) of CDAFA by knowingly and  
13 without permission accessing and using those devices and computer services, and/or causing them  
14 to be accessed and used, *inter alia*, in connection with Facebook's wrongful collection of such  
15 data.

16           333. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any  
17 set of computer instructions that are designed to . . . record, or transmit information within a  
18 computer, computer system, or computer network without the intent or permission of the owner  
19 of the information."

20           334. Defendant violated § 502(c)(8) by knowingly and without permission introducing  
21 a computer contaminant via Meta Pixel embedded into the Online Platforms which intercepted  
22 Plaintiff's and the Class Members' private and sensitive medical information.

23           335. Defendant's violation of the CDAFA caused Plaintiff and Class Members, at

1 minimum, the following damages:

- 2 a. Sensitive and confidential information that Plaintiff and Class Members  
3 intended to remain private is no longer private.
- 4 b. Defendant eroded the essential confidential nature of the doctor-patient  
5 relationship.
- 6 c. Defendant took something of value from Plaintiff and Class Members and  
7 derived benefit therefrom without Plaintiff's and Class Members'  
8 knowledge or informed consent and without sharing the benefit of such  
9 value;
- 10 d. Plaintiff and Class Members did not get the full value of the medical  
11 services for which they paid, which included Defendant's duty to maintain  
12 confidentiality; and
- 13 e. Defendant's actions diminished the value of Plaintiff's and Class Members'  
14 Private Information.

15 336. Plaintiff and the Class Members seek compensatory damages in accordance with  
16 Cal. Penal Code § 502(e)(1), in an amount to be proved at trial, and injunctive or other equitable  
17 relief; as well as punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) as  
18 Defendant's violations were willful and, upon information and belief, Defendant is guilty of  
19 oppression, fraud, or malice as defined in Cal. Civil Code § 3294; and reasonable attorney's fees  
20 under § 502(e)(2).

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

23

1 **COUNT X**  
2 **VIOLATION OF CAL. BUS. & PROF. CODE §§ 17200, ET SEQ.**  
3 **(On Behalf of Plaintiff and the Class)**

4 338. Plaintiff re-allege and incorporate the above allegations as if fully set forth herein.

5 339. Plaintiff, and Defendant are each a “person” under Cal. Bus. & Prof. Code § 17201.

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

8 341. Defendant’s business acts and practices are “unlawful” under the Unfair  
9 Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et. seq.* (the “UCL”) because, as alleged above,  
10 Defendant violated California common law, and other statutes and causes of action alleged herein.

11 342. Defendant engaged in unlawful acts and practices by imbedding the Pixel on its  
12 Websites, which tracks, records, and transmits Plaintiff’s and Class Members’ PHI/Private  
13 Information they disclose to Defendant in confidence via the Online Platforms and Website to  
14 third parties without Plaintiff’s and Class Members’ knowledge and/or consent, in violation of the  
15 California Invasion of Privacy Act (“CIPA”), Cal. Penal Code §§ 630, *et seq.*; the California  
16 Confidentiality of Medical Information Act (“CMIA”), CAL. CIVIL CODE §§ 56.06, 56.10,  
17 56.101; the Comprehensive Computer Data Access and Fraud Act (“CDAFA”), Cal. Penal Code  
18 § 502; and by representing that its services have characteristics, uses, or benefits that they do not  
19 have in violation of Civil Code § 1770.

20 343. When using Defendant’s Website and services, Plaintiff and Class Members relied  
21 on Defendant’s status as healthcare providers.

22 344. Inconsistent with its roles as a healthcare provider, Defendant disclosed Plaintiff’s  
23 and Class Members’ PHI/Private Information to third parties without their consent and for  
marketing purposes. Thus, Defendant represented that its services have characteristics, uses, or



1 benefits that they do not have and represented that its services are of a particular standard, quality,  
2 or grade when they were not, in violation of Cal. Civil Code § 1770.

3 345. Plaintiff and Class Members were reasonable to assume, and did assume, that  
4 Defendant would take appropriate measures to keep their PHI/Private Information secure and not  
5 share it with third parties without their express consent. Defendant also had a duty to disclose that  
6 they was sharing its patients' Personal Health Information with third parties. However, Defendant  
7 did not disclose at any time that they were sharing this PHI/Private Information with third parties  
8 via the Meta Pixel and other tracking technologies.

9 346. Had Plaintiff and Class Members known that Defendant would intercept, collect,  
10 and transmit their PHI/Private Information to Facebook and other third parties, Plaintiff and the  
11 Class Members would not have used Defendant's services.

12 347. Plaintiff and Class Members have a property interest in their PHI/Private  
13 Information. By surreptitiously collecting and otherwise misusing Plaintiff's and Class Members'  
14 PHI/Private Information, Defendant has taken property from Plaintiff and Class Members without  
15 providing just (or indeed any) compensation.

16 348. By deceptively collecting, using, and sharing Plaintiff's and Class Members'  
17 PHI/Private Information with Facebook and other third parties, Defendant have taken money or  
18 property from Plaintiff and Class Members. Accordingly, Plaintiff seek restitution on behalf of  
19 themselves and the Class.

20 349. Defendant's business acts and practices also meet the unfairness prong of  
21 California's Unfair Competition Law ("UCL") according to all three theories of unfairness.

22 350. First, Defendant's business acts and practices are "unfair" under the UCL pursuant  
23 to the three-part test articulated in *Camacho v. Automobile Club of Southern California* (2006) 142

1 Cal. App. 4th 1394, 1403: (a) Plaintiff and Class Members suffered substantial injury due to  
2 Defendant's Disclosure of their PHI/Private Information; (b) Defendant's disclosure of Plaintiff's  
3 and Class Members' PHI/Private Information provides no benefit to consumers, let alone any  
4 countervailing benefit that could justify Defendant's Disclosure of PHI/Private Information  
5 without consent for marketing purposes or other pecuniary gain; and (c) Plaintiff and Class  
6 Members could not have readily avoided this injury because they had no way of knowing that  
7 Defendant was implementing the Meta Pixel.

8 351. Second, Defendant's business acts and practices are "unfair" under the UCL  
9 because they are "immoral, unethical, oppressive, unscrupulous, or substantially injurious" to  
10 Plaintiff and Class Members, and "the utility of [Defendant's] conduct," if any, does not "outweigh  
11 the gravity of the harm" to Plaintiff and Class Members. *Drum v. San Fernando Valley Bar Ass'n*,  
12 (2010) 182 Cal. App. 4th 247, 257. Defendant secretly collected, disclosed, and otherwise misused  
13 Plaintiff's and Class Members' PHI/Private Information by bartering it to Facebook and other third  
14 parties in return for access to the Pixel tool. This surreptitious, willful, and undisclosed conduct is  
15 immoral, unethical, oppressive, unscrupulous, and substantially injurious. Moreover, no benefit  
16 inheres in this conduct, the gravity of which is significant.

17 352. Third, Defendant's business acts and practices are "unfair" under the UCL because  
18 they run afoul of "specific constitutional, statutory, or regulatory provisions." *Drum*, 182 Cal. App.  
19 4th at 256 (internal quotation marks and citations omitted). California has a strong public policy  
20 of protecting consumers' privacy interests, including consumers' and patients' personal data, as  
21 codified in California's Constitution in Article I, section 1; the California Invasion of Privacy Act  
22 ("CIPA"), Cal. Penal Code §§ 630, *et seq.*; the California Confidentiality of Medical Information  
23 Act ("CMIA"), Cal. Civil Code §§ 56.06, 56.10, 56.101; the Comprehensive Computer Data

1 Access and Fraud Act (“CDAFA”), Cal. Penal Code § 502, among other statutes.

2 353. Defendant violated this public policy by, among other things, surreptitiously  
3 collecting, disclosing, and otherwise exploiting Plaintiff and Class Members’ PHI/Private  
4 Information by sharing that information with Facebook and other third parties via the Tracking  
5 Pixel without Plaintiff’s and/or Class Members’ consent.

6 354. Had Plaintiff and Class Members known Defendant would intercept, collect, and  
7 transmit their PHI/Private Information to Facebook and other third parties, Plaintiff and Class  
8 Members would not have used Defendant’s services.

9 355. Plaintiff and Class Members were reasonable to assume, and did assume, that  
10 Defendant would take appropriate measures to keep their PHI/Private Information secure and not  
11 share it with third parties without their express consent. Defendant was in sole possession of and  
12 had a duty to disclose the material information that Patient Plaintiff’s and Class Members’ Personal  
13 Health Information would be shared with third parties via the Meta Pixel. Defendant did not  
14 disclose at any time that they were sharing this PHI/Private Information with third parties via the  
15 Tracking Pixel.

16 356. Plaintiff and Class Members have a property interest in their PHI/Private  
17 Information. By surreptitiously collecting and otherwise misusing Plaintiff’s and Class Members’  
18 Personal Health Information, Defendant has taken property from Plaintiff and Class Members  
19 without providing just (or indeed any) compensation.

20 357. Plaintiff and Class Members have lost money and property due to Defendant’s  
21 conduct in violation of the UCL. PHI/Private Information such as that which Defendant collected  
22 and transmitted to third parties has objective monetary value. Companies are willing to pay for  
23 PHI, like the information Defendant unlawfully collected and transmitted to third parties, such as

1 Facebook. For example, Pfizer annually pays approximately \$12 million to purchase health data  
2 from various sources.<sup>114</sup>

3 358. Consumers also value their personal health data. According to the annual Financial  
4 Trust Index Survey conducted by the University of Chicago's Booth School of Business and  
5 Northwestern University's Kellogg School of Management, which interviewed more than 1,000  
6 Americans, 93 percent of survey participants would not share their health data with a digital  
7 platform for free. Half of the survey participants would only share their data for \$100,000 or more,  
8 and 22 percent would only share their data if they received between \$1,000 and \$100,000.<sup>115</sup>

9 359. By deceptively collecting, using, and sharing Plaintiff's and Class Members'  
10 PHI/Private Information with Facebook and other third parties, Defendant has taken money and/or  
11 property from Plaintiff and Class Members. Accordingly, Plaintiff seek restitution on behalf of  
12 himself and the Class.

13 360. As a direct and proximate result of Defendant's unfair and unlawful methods and  
14 practices of competition, Plaintiff and Class Members suffered actual damages, including, but not  
15 limited to, the loss of the value of their Private Health Information.

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

22  
23 <sup>114</sup> <https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/>

<sup>115</sup> <https://www.beckershospitalreview.com/healthcare-information-technology/how-much-should-health-data-cost-100k-or-more-according-to-patients.html>

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, JOHN DOE, Individually, and on behalf of all others similarly situated, prays for judgment as follows:

- A. for an Order certifying this action as a Class action and appointing Plaintiff as Class Representatives and Plaintiff's counsel as Class Counsel;
- B. for an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- C. for an award of punitive damages, as allowable by law;
- D. for equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- E. for equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Private Information compromised and unlawfully disclosed to third parties;
- F. for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- G. an order that Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;
- H. for an award of attorneys' fees under the common fund doctrine, and any other applicable law;
- I. costs and any other expenses, including expert witness fees incurred by Plaintiff

1 in connection with this action;

2 J. pre- and post-judgment interest on any amounts awarded; and

3 K. such other and further relief as this court may deem just and proper.

4 **DEMAND FOR JURY TRIAL**

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

6 Dated: March 14, 2024

Respectfully submitted,

7 

8  
9 Vess A. Miller (278020)  
Natalie A. Lyons (293026)  
**COHEN & MALAD, LLP**  
One Indiana Square, Suite 1400  
Indianapolis, Indiana 46204  
(317) 636-6481  
nlyons@cohenandmalad.com  
vmiller@cohenandmalad.com

10  
11  
12  
13 Lynn A. Toops (*Pro Hac Vice* forthcoming)  
Mary Kate Dugan (*Pro Hac Vice* forthcoming)  
**COHEN & MALAD, LLP**  
One Indiana Square, Suite 1400  
Indianapolis, Indiana 46204  
(317) 636-6481  
ltoops@cohenandmalad.com  
mdugan@cohenandmalad.com

14  
15  
16  
17  
18 J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)  
Andrew E. Mize (*Pro Hac Vice* forthcoming)  
**STRANCH, JENNINGS & GARVEY, PLLC**  
The Freedom Center  
223 Rosa L. Parks Avenue, Suite 200  
Nashville, Tennessee 37203  
(615) 254-8801  
gstranch@stranchlaw.com  
amize@stranchlaw.com

19  
20  
21  
22  
23 Andrew Gunem (354042)  
**TURKE & STRAUSS, LLP**  
613 Williamson St., Suite 201

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

Madison, Wisconsin 53703  
(608) 237-1775  
[andrewg@turkestrauss.com](mailto:andrewg@turkestrauss.com)

*Counsel for Plaintiff and the Proposed Class*

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Lawsuit Claims Banner Health Website Visitors' Data Secretly Shared with Facebook, Google](#)

---