

1 Matthew J. Langley, California Bar No. 342846  
2 **ALMEIDA LAW GROUP LLC**  
3 849 W. Webster Avenue  
4 Chicago, Illinois 60614  
5 Tel: (312) 576-3024

6 *Attorneys for Plaintiffs & the Class*

7  
8 **UNITED STATES DISTRICT COURT**  
9 **NORTHERN DISTRICT OF CALIFORNIA**

10 CARLA MORENO AND FRANCES  
11 MORA, *individually and on behalf of all*  
12 *others similarly situated,*

13 *Plaintiffs,*

14 v.

15 QUANOVATE TECH INC. d/b/a MIRA,

16 *Defendant*

17 **Case No.**

- 18 1. VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. § 2511(1), *et seq.*;
- 19 2. NEGLIGENCE
- 20 3. VIOLATION OF FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, FLA. STAT. §§ 501.201, *et seq.*
- 21 4. VIOLATION OF FLORIDA SECURITY OF COMMUNICATIONS ACT (“FSCA”) FLA. STAT. § 934.01 *et seq.*
- 22 5. UNJUST ENRICHMENT
- 23 6. VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT, CAL. PENAL CODE §§ 630, *et seq.*

24 **JURY TRIAL DEMANDED**

1 **CLASS ACTION COMPLAINT**

2 Plaintiffs Carla Moreno and Frances Mora (“Plaintiffs”), individually and on behalf  
3 of all others similarly situated, by and through undersigned counsel, hereby allege the  
4 following against Quanovate Tech Inc. d/b/a Mira (“Mira” or “Defendant”). Facts  
5 pertaining to their experiences and circumstances are alleged based upon personal  
6 knowledge, and all other facts herein are alleged based on due investigation of counsel  
7 and—where indicated— upon information and good faith belief.

8 **NATURE OF THE ACTION**

9  
10 1. Defendant is a self-proclaimed “mini hormone lab” that offers both male  
11 and female customers at-home fertility testing and monitoring using quantitative  
12 technology.<sup>1</sup>

13 2. As alleged herein, Defendant engages in the illegal and widespread practice  
14 of disclosing Plaintiffs’ and putative Class Members’ confidential personally identifiable  
15 information (“PII”) and protected health information (“PHI”) (referred to herein  
16 collectively as “Private Information”) to third parties, including Meta Platforms, Inc. d/b/a  
17 Meta (“Facebook”) and Google LLC (“Google”) without its customers’ knowledge or  
18 consent.  
19

20 3. Information concerning a person’s physical and mental health is among the  
21 most confidential and sensitive information in our society and the mishandling of such  
22 information can have serious consequences including, but certainly not limited to,  
23 discrimination in the workplace and/or denial of insurance coverage.<sup>2</sup>  
24

25 \_\_\_\_\_  
26 <sup>1</sup> See <https://www.miracare.com/how-mira-works/> (last visited Aug. 14, 2024).

27 <sup>2</sup> See Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research*  
28 *found pervasive use of tracking tech on substance-abuse-focused health care websites,*  
*potentially endangering users in a post-Roe world* (Nov. 16, 2022),

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

6           5.       Reiterating the importance of and necessity for data security and privacy  
7 concerning health information, the Federal Trade Commission (“FTC”) recently published  
8 a bulletin entitled *Protecting the privacy of health information: A Baker’s dozen takeaways*  
9 *from FTC cases*, in which it noted that “[h]ealth information is not just about medications,  
10 procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables***  
11 ***an inference—about a consumer’s health.*** Indeed, [recent FTC enforcement actions  
12 involving] *Premom, BetterHelp, GoodRx and Flo Health make clear that the fact that a*  
13 ***consumer is using a particular health-related app or website—one related to mental***  
14 ***health or fertility, for example—or how they interact with that app (say, turning***  
15 ***‘pregnancy mode’ on or off) may itself be health information.***”<sup>3</sup>

16  
17  
18  
19  
20  
21  
22 <https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/> (last  
23 visited Aug. 14, 2024) (“While the sharing of any kind of patient information is often strictly  
24 regulated or outright forbidden, it’s even more verboten in addiction treatment, as patients’  
25 medical history can be inherently criminal and stigmatized.”); *see also* Todd Feathers,  
26 Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive*  
27 *Medical Information from Hospital Websites* (June 16, 2022), [https://themarkup.org/pixel-](https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites)  
28 [hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-](https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites)  
websites (last visited Aug. 14, 2024).

<sup>3</sup> *See* Elisa Jillison, *Protecting the privacy of health information: A Baker’s dozen*  
*takeaways from FTC cases* (July 25, 2023) (emphasis added), available at  
[https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-](https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases)  
[information-bakers-dozen-takeaways-ftc-cases](https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases) (last visited Aug. 14, 2024).

1           6.       The FTC is unequivocal in its stance as it informs—in no uncertain terms—  
2 healthcare companies that they should *not* use tracking technologies to collect sensitive  
3 health information and disclose it to various platforms without informed consent:

4           **Don't use behind-the-scenes tracking technologies that**  
5 **contradict your privacy promises or otherwise harm**  
6 **consumers.**

7           In today's surveillance economy, the consumer is often the  
8 product. Consumer data powers the advertising machine that  
9 goes right back to the consumer. *But when companies use*  
10 *consumers' sensitive health data for marketing and*  
11 *advertising purposes, such as by sending that data to*  
12 *marketing firms via tracking pixels on websites or software*  
13 *development kits on apps, watch out.*

14           [Recent FTC enforcement actions such as]  
15 *BetterHelp, GoodRx, Premom, and Flo* make clear that  
16 practices like that *may run afoul of the FTC Act if they violate*  
17 *privacy promises or if the company fails to get consumers'*  
18 *affirmative express consent for the disclosure of sensitive*  
19 *health information.*<sup>4</sup>

20           7.       The incontrovertible need for data security and transparency is particularly  
21 acute when it comes to the rapidly expanding worlds of telehealth and the sale of diagnostic  
22 test kits.

23           8.       Garnering wide-spread adaptation during the COVID-19 pandemic, these  
24 self-collection or at-home testing kits form an important part of consumers' access to  
25 healthcare by removing the impediments of having to travel to visit with medical providers.

26           9.       Despite testing for extremely sensitive and personal health issues relating  
27 to sexual and reproductive health, many of these at-home test kit retailers appear to value  
28

---

26 <sup>4</sup> *Id.* (emphasis added) (further noting that *GoodRx & Premom* underscore that this conduct  
27 may also violate the Health Breach Notification Rule, which requires notification to  
28 consumers, the FTC and, in some cases, the media, of disclosures of health information  
without consumers' authorization.

1 the collection and monetization of user data over all else.<sup>5</sup> The universe of data that these  
2 companies collect is vast as at-home test providers (and the laboratories with which they  
3 partner) can collect personal and health data on their customers through several channels,  
4 including through an initial online symptom survey, purchase information, customer  
5 interactions with provider websites or apps, and test results.<sup>6</sup>

6 10. Unfortunately, the process of searching for, researching, purchasing and  
7 using these kits is *not* as confidential a process as the retailers of these kits represent.

8 11. An investigation by THE MARKUP and KFF HEALTH NEWS found that many  
9 of the websites by which retailers advertised and sold these kits used certain tracking  
10 technologies to collect and to share confidential and protected health information with the  
11 biggest social media and advertising platforms, including Facebook and Instagram.<sup>7</sup>

12 12. That investigation found that “trackers collecting browsing- and purchase-  
13 related data on websites on 12 of the biggest drugstores in the United States, including  
14 grocery store chains with pharmacies, and sharing the sensitive information with companies  
15 like Meta and Google, through their advertising and analytics products and Microsoft,  
16 through its search engine, Bing.”<sup>8</sup>

17  
18  
19  
20  
21  
22 <sup>5</sup> See, e.g., *Top Mental Health & Prayer Apps Fail Spectacularly at Privacy, Security* (May  
23 2, 2022), <https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security/> (last visited Aug. 14, 2024).

24 <sup>6</sup> As noted by the FTC, at-home test kit providers should be upfront with customers about  
25 what data they collect, how it is stored and with whom it is shared.

26 <sup>7</sup> See Danielle Ellis, *Need to get Plan B or an HIV test online? Facebook may know about*  
27 *it*, KFF HEALTH NEWS & THE MARKUP (June 30, 2023),  
<https://kffhealthnews.org/news/article/drugstores-pixel-sensitive-data-social-media-companies/> (last visited Aug. 14, 2024).

28 <sup>8</sup> *Id.*

1           13.       Rather than attempt to collect more and more confidential and protected  
2 health information, telehealth and diagnostic test kit companies should minimize data  
3 collection and storage to what is necessary to provide health care services. In practice, few  
4 do; rather, likely cognizant that consumers would not voluntarily provide this sensitive and  
5 protected information, these companies resort to doing so covertly by installing invisible  
6 tracking technologies on their websites to collect and monetize that data.<sup>9</sup>  
7

8           14.       Moreover, many companies do not publicly disclose what types of data they  
9 disclose—for instance, contact information or aspects of their health data. By disclosing  
10 customer data to third parties and providing little transparency into what data is shared and  
11 with whom, test providers make it more likely that sensitive data could be leaked, used to  
12 discriminate, and/or sold (and re-sold) by data brokers without oversight or consent.<sup>10</sup>  
13

14           15.       These companies—including Defendant—are facilitating their surreptitious  
15 connection and disclosure of protected health and other information by using invisible  
16 tracking tools, including those popularly called “pixels.”

17           16.       Defendant’s unlawful privacy violations occurred and continue to occur  
18 because of the tracking technologies that it installed on its website including, but not limited  
19 to, the Meta Pixel, Google Analytics, Google DoubleClick and Google Tag Manager  
20 (collectively, “Tracking Tools”).<sup>11</sup>  
21

---

22 <sup>9</sup> See, *supra*, n.2. Moreover, the policies of many test providers fail to include specific  
23 limitations around data retention and deletion, instead relying on vague, catchall language.

24 <sup>10</sup> Kaylana Mueller-Hsia & Laura Hecht-Fellala, *Evaluating the Privacy of At-Home Covid*  
25 *19 Tests, The Tests Are Essential for Fighting the Pandemic, but Poor Privacy Policy*  
26 *Practices Could Discourage Some People from Using Them*, BRENNAN CENTER FOR  
27 JUSTICE (Jan. 19, 2021), available at <https://www.brennancenter.org/our-work/analysis-opinion/evaluating-privacy-covid-19-home-tests#:~:text=To%20maximize%20privacy%20protections%2C%20test,however%2C%20adhere%20to%20these%20principles> (last visited Aug. 14, 2024).

28 <sup>11</sup> While this Complaint focuses on tracking tools from Facebook and Google, research

1           17.     Invisible to the naked eye, each of the Pixels embedded on Defendant's  
2 Website collects and transmits information from Users' (defined below) browsers to  
3 unauthorized third parties including, but not limited to, Facebook, Google, and other third-  
4 party data brokers (collectively, the "Pixel Information Recipients").

5           18.     The Pixel Information Recipients, in turn, use Plaintiffs' and Class  
6 Members' Private Information for business purposes, including to improve advertisers'  
7 ability to target specific demographics and selling such information to third-party marketers  
8 who target Plaintiffs and Class Members online (*i.e.*, through their Facebook, Instagram,  
9 Gmail and other social media and personal accounts) with targeted advertising related to  
10 the PHI they shared with companies like Defendant.

11           19.     For example, in the case of information sent by Mira to Facebook, such  
12 information was then linked to Plaintiffs' unique Facebook user ID ("Facebook ID" or  
13 "FID") so that there was no anonymity; Facebook and/or any third parties who were able  
14 to access the information could directly associate such personal health information with  
15 Plaintiffs and each of the Class Members.<sup>12</sup>

16           20.     Simply put, the Pixels secretly enable the unauthorized transmission and  
17 disclosure of Plaintiffs' and Class Members' highly sensitive Private Information by  
18 Defendant. To begin, these websites' pixels send several unique personal identifiers,  
19 including a User's Facebook ID to social media giants and other firms.  
20  
21  
22

23 \_\_\_\_\_  
24 shows that Defendant also embedded tracking codes from a number of other marketing  
25 companies including Bing (Microsoft), Clarity (Microsoft), LinkedIn, Pinterest, and Yahoo.

26 <sup>12</sup> Regardless, Facebook tracks and collects data even on people who don't have a Facebook  
27 account or have deactivated their Facebook accounts. They can be in an even worse  
28 situation since the data is being collected about them but, because they don't have an  
account (or an active account), they cannot clear past activity or disconnect the collection  
of future activity. In the past, these were referenced as "ghost accounts" or "shadow  
profiles."

1           21.       They also send cookies – a way of storing information in a user’s browser  
2 that helps track a user from page to page as the user browses a retailer’s site.<sup>13</sup>

3           22.       In addition to the IP address, Facebook ID, cookies and other personally  
4 identifying information, the Pixels send sensitive information about what items a consumer  
5 has viewed, clicked and purchased.

6           23.       Defendant Mira, which sells fertility test kits for private at-home testing as  
7 well as other health and wellness products for at-home consumption, is one such company.

8           24.       In order to provide these services, Mira owns, controls and maintains the  
9 website <https://www.miracare.com/> (referred to herein as the “Website”), which requires  
10 individuals to provide Private Information in order to create accounts and to participate in  
11 highly sensitive and personal health screenings and to view and to purchase diagnostic kits,  
12 among other things.

13           25.       Plaintiffs and Class Members who visited and used Mira’s Website  
14 (collectively, the “Users”) understandably thought they were communicating *only* with their  
15 trusted healthcare provider. Unfortunately, Mira intentionally chose to put its profits over  
16 the privacy of its Users.

17           26.       Plaintiffs therefore brings this class action lawsuit to address Mira’s  
18 transmission and disclosure of Plaintiffs’ and Class Members’ Private Information to  
19 Facebook, Google, and other third parties via tracking pixels (“Meta Pixel” or “Pixel”) and  
20 other tracking technologies installed on Defendant’s Website.

21           27.       This case concerns a very serious breach of Mira’s data privacy and security  
22 obligations as it installed these tracking technologies on its Website to collect and to  
23

24  
25  
26  
27  
28 <sup>13</sup> Cookies are often also used to associate individuals on a site with their account on a social  
media platform, such as Facebook or Instagram.



1 disclose to unauthorized third parties Plaintiffs' and Class Members' Private Information  
2 for the purpose of disclosing that information to Meta, Google and other third parties, in  
3 violation of HIPAA and common law.

4 28. Plaintiffs and Class Members reasonably expected that their healthcare-  
5 related communications with Mira via its Website were confidential, solely between  
6 themselves and Mira and that such communications would not be disclosed to or intercepted  
7 by a third party.

8  
9 29. Plaintiffs and Class Members would *not* have provided their sensitive  
10 Private Information to Mira had they known that Defendant would disclose it to  
11 unauthorized third parties.

12 30. As evidenced by, among other things, the fact that companies are  
13 endeavoring to acquire Plaintiffs' and Class Members' Private Information, that  
14 information unquestionably has value as companies like Facebook utilize the precise type  
15 of information disclosed by Defendant to identify, target and market products and services  
16 to individuals.

17  
18 31. Additionally, and upon information and good faith belief, Mira  
19 surreptitiously collects Plaintiffs' and Class Members' Private Information to use it for  
20 retargeting, a form of online marketing that targets users with ads based on their previous  
21 Internet communications and interactions.

22  
23 32. What Mira has not publicly acknowledged is that customers would be  
24 unknowingly sacrificing their privacy by using its Website. That is, Mira made the  
25 conscious and intentional decision to put its profits over the privacy of its Users.

26 33. When Plaintiffs and other customers used Defendant's Website in order to  
27 search for and obtain fertility test kits, the names and types of such test kits were secretly  
28

1 disclosed to Facebook, Google and other unauthorized third parties, along with the  
2 customers' personal information and personal identifiers.

3 34. As detailed herein, Mira's privacy policy provided no warning whatsoever  
4 that Class Members' PHI and/or other sensitive personal and health information would be  
5 disclosed to Facebook and other unauthorized third parties for marketing purposes or  
6 otherwise. Rather, the applicable privacy policies stated that Mira would only use Plaintiffs'  
7 and Class Members' information "in order to provide you the services you have requested,  
8 process your order, and respond to any order or billing related questions."<sup>14</sup>  
9

10 35. Mira *never* obtained such authorizations from Plaintiffs or the Class  
11 Members. At all times relevant to this action, Plaintiffs and Class Members had no informed  
12 consent that information about their sensitive health conditions would be transmitted to the  
13 largest social media company on earth, which has a sordid history of privacy violations in  
14 pursuit of ever-increasing advertising revenue.  
15

16 36. Upon information and belief, Mira also installed and implemented the  
17 Facebook Conversions Application Programming Interface ("Conversions API") on the  
18 Website. Conversions API serves the same purpose as the Pixels in that it surreptitiously  
19 collects and transmits Private Information to Facebook. Unlike the Pixels, however,  
20 Conversions API functions from Defendant's servers and therefore cannot be stymied by  
21 use of anti-Pixel software or other workarounds. Mira secretly enabled additional  
22 unauthorized transmissions and disclosures of Plaintiffs' and Class Members' Private  
23 Information to Facebook by implementing the Conversions API.  
24

25 37. Thus, operating as implemented by Mira, the Pixels, Conversions API and  
26 other tracking technologies allow the Private Information that Plaintiffs and Class Members  
27

28 <sup>14</sup> See Defendant's *Privacy Policy*, <https://www.miracare.com/privacy-policy/>.

1 submit in confidence to be unlawfully disclosed to Facebook alongside the individual's  
2 name and other identifying information, including his or her Facebook ID, IP addresses and  
3 other identifying information pertaining to any accounts they may have with Facebook. This  
4 surreptitious and illegal collection and divulgence occurs on every webpage in which Mira  
5 installed the Pixels and for which it enabled Conversions API.

6  
7 38. Despite warnings that healthcare companies were disclosing Private  
8 Information to social media companies by embedding and using Pixels and/or similar  
9 tracking technologies as far back as at least February 2020, Mira breached confidentiality  
10 and violated Plaintiffs' and Class Members' privacy when it chose to embed the Pixels and  
11 other tracking codes to share Private Information with third parties.<sup>15</sup>

12  
13 39. As detailed herein, Mira owed common law, statutory and regulatory duties  
14 to keep Plaintiffs' and Class Members' communications and medical information safe,  
15 secure and confidential. First, the disclosure of Plaintiffs' and Class Members' Private  
16 Information via the Pixels contravenes the letter and spirit of HIPAA's "Standards for  
17 Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule")  
18 which governs how health care providers must safeguard and protect Private Information.

19  
20 40. While healthcare organizations regulated under HIPAA may use third-party  
21 tracking tools, such as Google Analytics or Meta Pixel, they can do so only in a very limited  
22 way:

23 Identifying information alone, such as personal names, residential  
24 addresses, or phone numbers, would not necessarily be designated  
25 as PHI. For instance, if such information was reported as part of a

24  
25 <sup>15</sup> Molly Osberg & Dhruv Mehrotra, *The Spooky, Loosely Regulated World of Online*  
26 *Therapy*, JEZEBEL (Feb. 19, 2020), [https://jezebel.com/the-spooky-loosely-regulated-](https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137)  
27 [world-of-online-therapy-1841791137](https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137) (last visited Aug. 14, 2024); *see also* Timothy M.  
28 Hale, PhD & Joseph C. Kvedar, MD, *Privacy and Security Concerns in Telehealth* (Dec.  
2014), [https://journalofethics.ama-assn.org/article/privacy-and-security-concerns-](https://journalofethics.ama-assn.org/article/privacy-and-security-concerns-telehealth/2014-12)  
[telehealth/2014-12](https://journalofethics.ama-assn.org/article/privacy-and-security-concerns-telehealth/2014-12), *AMA JOURNAL OF ETHICS* (illustrating that problems with privacy and  
telehealth apps started to surface as early as 2014) (last visited Aug. 14, 2024).

1 publicly accessible data source, such as a phone book, then this  
 2 information would not be PHI because it is not related to health  
 3 data... ***If such information was listed with health condition, health  
 4 care provision, or payment data, such as an indication that the  
 5 individual was treated at a certain clinic, then this information  
 6 would be PHI.***<sup>16</sup>

7 41. Moreover, the Office for Civil Rights at HHS has made clear, in a recent  
 8 bulletin titled Use of Online Tracking Technologies by HIPAA Covered Entities and  
 9 Business Associates, that the transmission of such protected information violates HIPAA's  
 10 Privacy Rule:

11 **Regulated entities are not permitted to use tracking technologies  
 12 in a manner that would result in impermissible disclosures of  
 13 PHI to tracking technology vendors or any other violations of  
 14 the HIPAA Rules.** For example, disclosures of PHI to tracking  
 15 technology vendors for marketing purposes, without individuals'  
 16 HIPAA-compliant authorizations, would constitute impermissible  
 17 disclosures.<sup>17</sup>

18 <sup>16</sup> *Guidance regarding Methods for De-identification of Protected Health Information in  
 19 Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy  
 20 Rule,* [https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-  
 21 identification/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html) (last visited Aug. 14, 2024) (noting that "HIPAA Identifiers"  
 22 include name; address (all geographic subdivisions smaller than state, including street  
 23 address, city county, and zip code); all elements (except years) of dates related to an  
 24 individual (including birthdate, admission date, discharge date, date of death, and exact  
 25 age); telephone numbers; email address; medical record number; health plan beneficiary  
 26 number; account number; device identifiers and serial numbers; web URL; internet protocol  
 27 (IP) address; and any other characteristic that could uniquely identify the individual).

28 <sup>17</sup> *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business  
 Associates,* Dept. of Health and Human Services, [https://www.hhs.gov/hipaa/for-  
 professionals/privacy/guidance/hipaa-online-tracking/index.htm](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.htm) (noting that "IIHI  
 collected on a regulated entity's website or mobile app generally is PHI, even if the  
 individual does not have an existing relationship with the regulated entity and even if the  
 IIHI, such as in some circumstances IP address or geographic location, does not include  
 specific treatment or billing information like dates and types of health care services."").  
 This guidance was recently vacated *in part* by the Federal District Court for the Northern  
 District of Texas due to the court finding it in part to be the product of improper  
 rulemaking and it is cited for reference only until the OCR updates its guidance, should it  
 do so in the future. *See American Hosp. Ass'n. v. Becerra*, No. 4:23-cv-01110-P, ECF No.  
 67 (S.D. Tex., Jun. 20, 2024). Notably, the court's order found only that the OCR's  
 guidance regarding covered entities disclosing to third parties users' IP addresses while  
 users navigated *unauthenticated public webpages* ("UPWs") was improper rulemaking.

1           42. Further, Mira breached its statutory and common law obligations to  
2 Plaintiffs and Class Members by, *inter alia*: (i) failing to adequately review its marketing  
3 programs to ensure its Website was safe and secure; (ii) failing to remove or disengage  
4 technology that was known and designed to share Users' Private Information; (iii) failing  
5 to obtain the prior written consent of Plaintiffs and Class Members to disclose their Private  
6 Information to Facebook and other unauthorized third parties before doing so; (iv) failing  
7 to take steps to block the transmission of Plaintiffs' and Class Members' Private  
8 Information through the Pixels; (v) failing to warn Plaintiffs and Class Members that their  
9 Private Information was being shared with third parties without express consent and (vi)  
10 otherwise failing to design and monitor its Website to maintain the security, confidentiality  
11 and integrity of customer Private Information.  
12

13           43. Despite incorporating the Pixels, Conversions API, and other third-party  
14 tracking technologies into its Website and servers, Mira has never disclosed to Plaintiffs or  
15 Class Members that it shared their sensitive and confidential communications and Private  
16 Information with Facebook.<sup>18</sup>  
17

18 \_\_\_\_\_  
19 The Order in no way affects or undermines the OCR's guidance regarding covered entities  
20 disclosing personal identifiers, such as Google or Facebook identifiers, to third parties  
21 while patients were making appointments for particular conditions, paying medical bills  
22 or logging into (or using) a patient portal. *See id.* at 3-4, 31, n. 8 (vacating the OCR  
23 guidance with respect to the "Proscribed Combination" defined as "circumstances where  
24 an online technology connects (1) an individual's IP address with (2) a visit to a UPW  
25 addressing specific health conditions or healthcare providers" but stating that "[s]uch  
26 vacatur is not intended to, and should not be construed as, limiting the legal operability of  
27 other guidance in the germane HHS document."). Furthermore, the FTC bulletin on the  
28 same topics remains untouched, as do the FTC's enforcement actions against healthcare  
providers for committing the same actions alleged herein).

<sup>18</sup> In contrast to Defendant, in recent months several medical providers which have installed  
the Facebook Pixel on their web properties have provided their patients with notices of data  
breaches caused by the Pixels transmitting PHI to third parties. *See, e.g., Cerebral, Inc.*  
*Notice of HIPAA Privacy Breach*, [https://cerebral.com/static/hippa\\_privacy\\_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf](https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf); *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies* (Oct. 20, 2022),









1 58. Plaintiff Moreno had an active Facebook account while she used  
2 Defendant's services, and she accessed Defendant's Website while logged into her  
3 Facebook account on the same device.

4 59. Defendant transmitted Plaintiff Moreno's Facebook ID, computer IP  
5 address and other device and unique online identifiers to Facebook. Defendant also  
6 transmitted information such as health and medical information including Plaintiff's  
7 particular health condition and the type of medical testing sought such as fertility tests and  
8 supplements.  
9

10 60. After providing her Private Information to Defendant through the Website,  
11 Plaintiff Moreno immediately began seeing targeted ads related to fertility and pregnancy  
12 on her Facebook account.

13 61. Upon information and good faith belief, Plaintiff began receiving these ads  
14 after her Private Information was disclosed by Defendant's Pixel to Facebook, which  
15 accessed and analyzed that information to identify Plaintiff's Facebook account and  
16 determine which advertisements would most effectively target her medical condition (in  
17 this case, fertility issues and attempts to conceive). Facebook, in turn, shared the  
18 information with other unauthorized third parties so that they could determine if their ads  
19 would effectively target that condition.  
20

21 62. The full scope of Defendant's interceptions and disclosures of Plaintiff's  
22 communications to Meta can only be determined through formal discovery. However,  
23 Defendant intercepted at least the following communications about Plaintiff's medical  
24 condition, diagnosis, and testing, via descriptive long-URLs that were sent to Meta via the  
25 Pixel and which contained information concerning Plaintiffs' specific medical conditions,  
26 and testing sought  
27  
28

1           63. Plaintiff Moreno would not have utilized Defendant's services and products  
2 and/or used its Website, or would have paid much less for Defendant's services and  
3 products, had she known that her Private Information would be captured and disclosed to  
4 third parties like Facebook and Google without her consent.

5           64. Plaintiff was injured by Defendant's unauthorized disclosure of her  
6 confidential medical information. Defendant's actions subjected her to unsolicited targeted  
7 advertising related to her specific medical conditions and caused significant mental distress  
8 arising from the implication that advertisers were aware of her medical conditions and the  
9 fear that her friends, family, or colleagues might see these advertisements and thereby learn  
10 of her medical conditions. Additionally, Defendant's practice of sharing Plaintiff's Private  
11 Information has diminished the value of the disclosed Private Information.  
12

13           65. Plaintiff Moreno has a continuing interest in ensuring that her Private  
14 Information, which, upon information and belief, remains backed up in Defendant's  
15 possession, is protected and safeguarded from future unauthorized disclosure(s).  
16

17           **Plaintiff Mora**

18           66. Plaintiff Mora began utilizing Defendant's Website starting at least in June  
19 2020 on her personal electronic devices to research and purchase at-home fertility test kits,  
20 including those offered for sale by Defendant on its Website.

21           67. Specifically, Plaintiff Mora has purchased at-home fertility test products  
22 such as Mira Fertility Starter Kit and Mira Fertility Replacement Test Wands in June 2020,  
23 and Mira Estrogen+LH Replacement Test Wands in December 2020 and April 2021 from  
24 Mira's Website.  
25  
26  
27  
28

1           68.     While researching and purchasing these products, Mira required Plaintiff to  
2 provide—and Plaintiff provided—Private Information including personal health  
3 information.

4           69.     Plaintiff Mora reasonably expected that her communications with  
5 Defendant via the Website were confidential, solely between herself and Defendant, and  
6 that such communications would not be transmitted to or intercepted by a third party.

7  
8           70.     Plaintiff Mora never consented to or authorized Defendant to disclose her  
9 Private Information to third parties or for Defendant to enable third parties to access,  
10 interpret and use such Private Information.

11           71.     Plaintiff Mora had an active Facebook account while she used Defendant’s  
12 services, and she accessed Defendant’s Website while logged into her Facebook account on  
13 the same device.

14           72.     Defendant transmitted Plaintiff Mora’s Facebook ID, computer IP address  
15 and other device and unique online identifiers to Facebook. Defendant also transmitted  
16 information such as health and medical information including Plaintiff’s particular health  
17 condition and the type of medical testing sought.

18  
19           73.     After providing her Private Information to Defendant through the Website,  
20 Plaintiff Mora immediately began seeing targeted ads related to fertility and pregnancy on  
21 her Facebook account.

22  
23           74.     Upon information and good faith belief, Plaintiff began receiving these ads  
24 after her Private Information was disclosed by Defendant’s Pixel to Facebook, which  
25 accessed and analyzed that information to identify Plaintiff’s Facebook account and  
26 determine which advertisements would most effectively target her medical condition (in  
27  
28

1 this case, infertility). Facebook, in turn, shared the information with other unauthorized  
2 third parties so that they could determine if their ads would effectively target that condition.

3 75. The full scope of Defendant's interceptions and disclosures of Plaintiff's  
4 communications to Meta can only be determined through formal discovery. However,  
5 Defendant intercepted at least the following communications about Plaintiff's medical  
6 condition, diagnosis, and testing, via descriptive long-URLs that were sent to Meta via the  
7 Pixel and which contained information concerning Plaintiff's specific medical conditions  
8 as well as testing sought, such as her purchases of fertility test kits and supplements.  
9

10 76. Plaintiff Mora would not have utilized Defendant's services and products  
11 and/or used its Website, or would have paid much less for Defendant's services and  
12 products, had she known that her Private Information would be captured and disclosed to  
13 third parties like Facebook and Google without her consent.

14 77. Plaintiff was injured by Defendant's unauthorized disclosure of her  
15 confidential medical information. Defendant's actions subjected her to unsolicited targeted  
16 advertising related to her specific medical conditions and caused significant mental distress  
17 arising from the implication that advertisers were aware of her medical conditions and the  
18 fear that her friends, family, or colleagues might see these advertisements and thereby learn  
19 of her medical conditions. Additionally, Defendant's practice of sharing Plaintiff's Private  
20 Information has diminished the value of the disclosed Private Information.  
21

22 78. Plaintiff Mora has a continuing interest in ensuring that her Private  
23 Information, which, upon information and belief, remains backed up in Defendant's  
24 possession, is protected and safeguarded from future unauthorized disclosure(s).  
25

## 26 **FACTUAL ALLEGATIONS**

### 27 **I. THE USE OF TRACKING PIXELS IN THE HEALTHCARE INDUSTRY.**

28

1           79.     A “pixel” is a piece of code that “tracks the people and the types of actions  
2 they take”<sup>19</sup> as they interact with a website, including how long a person spends on a  
3 particular webpage, which buttons the person clicks, which pages they view, the text or  
4 phrases they type into various portions of the website (such as a general search bar, chat  
5 feature, or text box) and much, much more.

6           80.     When embedded on a company’s website, the Pixels send data about user  
7 activity, including what you are viewing, your searches on websites, purchases you have  
8 made, items added to a shopping cart, and even information you filled out in online forms.<sup>20</sup>  
9 Meta calls this activity “interactions.”

10           81.     Pixels send this information back to Facebook even if the User does not have  
11 a Facebook account. The website publishers can then use this information to retarget Users  
12 by advertising their products when they are on a Meta property or through the Meta Audience  
13 Network for non-Meta websites and mobile apps.

14           82.     Pixels are routinely used to target specific customers by utilizing data to  
15 build profiles for the purposes of retargeting—*i.e.*, serving online advertisements to people  
16 who have previously engaged with a business’s website—and other marketing.

17           83.     Here, a user’s web browser executes the Pixels via instructions within each  
18 webpage of Defendant’s Website to communicate certain information (within parameters  
19 set by Defendant) directly to the corresponding Pixel Information Recipients.  
20  
21  
22  
23  
24

---

25 <sup>19</sup> *Retargeting*, <https://www.facebook.com/business/goals/retargeting> (last visited Aug. 14,  
26 2024).

27 <sup>20</sup> See Tom Kemp, “*Oops! I Did It Again*” ... *Meta Pixel Still Hoovering Up Our Sensitive*  
28 *Data* (July 2, 2023), <https://tomkemp00.medium.com/oops-i-did-it-again-meta-pixel-still-hoovering-up-our-sensitive-data-f99c7b779d47> (last visited Aug. 14, 2024).

1 84. The Pixels can also share the user’s identifying information for easy  
2 tracking via the “cookies”<sup>21</sup> stored on their computer by any of the Pixel Information  
3 Recipients with which they have an account.

4 85. For example, Facebook stores or updates a Facebook-specific cookie every  
5 time a person accesses their Facebook account from the same web browser. The Facebook  
6 Pixel can access this cookie and send certain identifying information like the user’s  
7 Facebook ID to Facebook along with the other data relating to the user’s Website inputs.  
8 The same is true for the other Pixel Information Recipients, which also create cookies that  
9 are stored in the user’s computer and accessed by the Pixels to identify the user.  
10

11 86. The Pixels are programmable, meaning that Defendant controls which of  
12 the webpages on the Website contain the Pixels, and which events are tracked and  
13 transmitted to the Pixel Information Recipients.

14 87. Defendant used the data it collected from Plaintiffs and Class Members,  
15 without their consent, to improve their advertising and bolster its revenues.  
16

17 **II. IN ORDER FOR PLAINTIFFS & CLASS MEMBERS TO PURCHASE**  
18 **HEALTHCARE PRODUCTS ON ITS WEBSITE, DEFENDANT**  
19 **REQUIRED THEIR PRIVATE INFORMATION TO BE COLLECTED &**  
20 **STORED ON ITS WEBSITE.**

21 88. Throughout the Class Period, Defendant maintained and operated the  
22 Website, by and through which Defendant encouraged and permitted consumers to research  
23 and purchase healthcare products.  
24  
25

---

26 <sup>21</sup> “Cookies are small files of information that a web server generates and sends to a web  
27 browser Cookies help inform websites about the user, enabling the websites to personalize  
28 the user experience.” See <https://www.cloudflare.com/learning/privacy/what-are-cookies/>  
last visited Aug. 14, 2024).

1 89. To purchase sensitive healthcare products, including fertility testing kits,  
2 Plaintiffs and other Class Members were required to search for and to add the healthcare  
3 products to their virtual cart before proceeding to checkout.

4 90. Each step of this process was tracked and logged by the Meta Pixel.  
5 Throughout the Class Period, the process for purchasing healthcare products on the Website  
6 has been substantially the same in all material respects throughout the United States.

7  
8 91. Thus, in order to use the Website to purchase healthcare products, including  
9 fertility test kits, Plaintiffs and other Class Members were required by Defendant to disclose  
10 confidential, private, and sensitive personal and health information to Defendant, and to  
11 have that information stored on Defendant's website servers along with their personal  
12 identifiers.

13 **III. DEFENDANT SECRETLY DISCLOSED & PERMITTED THIRD**  
14 **PARTIES TO INTERCEPT PLAINTIFFS' & CLASS MEMBERS'**  
15 **PRIVATE INFORMATION.**

16 92. Unbeknownst to Plaintiffs and other Class Members, the Private  
17 Information that they communicated to Defendant through the Website while purchasing  
18 healthcare products was intercepted by and/or disclosed to third parties including Facebook  
19 and Google.

20 **A. Defendant's Use of the Pixels, Source Code & Interception of HTTP**  
21 **Requests**

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

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

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

- 8 • **HTTP Request:** an electronic communication sent from the client device’s  
9 browser to the website’s server. GET Requests are one of the most common  
10 types of HTTP Requests. In addition to specifying a particular URL (i.e., web  
11 address), GET Requests can also send data to the host server embedded inside  
12 the URL, and can include cookies.
- 13 • **Cookies:** a small text file that can be used to store information on the client  
14 device which can later be communicated to a server or servers. Cookies are  
15 sent with HTTP Requests from client devices to the host server. Some  
16 cookies are “third-party cookies” which means they can store and  
17 communicate data when visiting one website to an entirely different website.
- 18 • **HTTP Response:** an electronic communication that is sent as a reply to the  
19 client device’s web browser from the host server in response to an HTTP  
20 Request. HTTP Responses may consist of a web page, another kind of file,  
21 text information, or error codes, among other data.<sup>22</sup>

22 96. A customer’s HTTP Request essentially asks the Website to retrieve certain  
23 information (such as sensitive healthcare products placed in the virtual shopping cart), and  
24 the HTTP Response renders or loads the requested information in the form of “Markup”  
25 (the pages, images, words, buttons, and other features that appear on the customer’s screen  
26 as they navigate the Website).

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

---

<sup>22</sup> One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.



1           98.       Source code may also command a web browser to send data transmissions  
2 to third parties in the form of HTTP Requests quietly executed in the background without  
3 notifying the user. The Pixels and other tracking technologies Defendant installed constitute  
4 source code that does just that. These tracking technologies thus act much like a traditional  
5 wiretap.

6           99.       Defendant encourages customers to use its Website to purchase fertility test  
7 kits and take other actions related to their personal medical conditions. When interacting  
8 with Defendant’s Website like this, Plaintiffs and Class Members convey highly private  
9 and sensitive information to Defendant.

10           100.      When customers visit Defendant’s Website via an HTTP Request to  
11 Defendant’s server, that server sends an HTTP Response including the Markup that displays  
12 the webpage visible to the user and Source Code, including the Pixels being utilized by  
13 Defendant to track its customers’ every move.

14           101.      Thus, Defendant is in essence handing customers a tapped device, and once  
15 the webpage is loaded into the customer’s browser, the software-based wiretap is quietly  
16 waiting for private communications on the Website to trigger the tap, which intercepts those  
17 communications intended only for Defendant and transmits those communications to third  
18 parties, including Facebook, Google, Bing, Clarity, Yahoo and others.

19           102.      Third-parties, like Facebook and Google, place third-party cookies in the  
20 web browsers of users logged into their services. These cookies uniquely identify the user  
21 and are sent with each intercepted communication to ensure the third party can uniquely  
22 identify the customer associated with the Private Information intercepted.

23           103.      Defendant intentionally configured Pixels installed on its Website to  
24 capture both the “characteristics” of individual customers’ communications with the  
25

1 Defendant's Website (e.g., their IP addresses, Facebook ID, cookie identifiers, device  
2 identifiers and account numbers) and the "content" of these communications (i.e., the  
3 buttons, links, pages, and tabs they click and view, as well as search terms entered into free  
4 text boxes and descriptive URLs showing the information being exchanged).

5           104. Defendant also deposits cookies named `_fbp` and `_ga` onto Plaintiffs' and  
6 Class Members' computing devices. These are cookies associated with the third-parties  
7 Facebook and Google but which Defendant deposits on Plaintiffs' and Class Members'  
8 computing devices by disguising them as first-party cookies. Without any action or  
9 authorization, Defendant commands Plaintiffs' and Class Members' computing devices to  
10 contemporaneously re-direct the Plaintiffs' and Class Members' identifiers and the content  
11 of their communications to Facebook and Google.

12           105. The `fbp` cookie is a Facebook identifier that is set by Facebook source code  
13 and associated with Defendant's use of the Facebook Meta Pixel program. The `fbp` cookie  
14 emanates from Defendant's Website as a putative first party cookie but is transmitted to  
15 Facebook through cookie synching technology that hacks around the same-origin policy.  
16 The `_ga` cookie operates similarly as to Google.

17           106. Furthermore, if the customer is also a Facebook user, the information  
18 Facebook receives is linked to the customer's Facebook profile (via their Facebook ID or  
19 "c\_user id"), which includes other identifying information.

20           107. The third parties to whom a website transmits data through pixels and  
21 associated workarounds do not provide any substantive content relating to the user's  
22 communications. Instead, these third parties are typically procured to track user data and  
23 intercept their communications for the marketing purposes of the website owner.  
24  
25  
26  
27  
28

1           108. Thus, without any knowledge, authorization, or action by a user, a website  
2 owner like Defendant can use its source code to commandeer a user’s computing device,  
3 causing the device to contemporaneously and invisibly re-direct the users’ communications  
4 to third parties.

5           109. In this case, Defendant employed just such devices (the Meta Pixel, Google  
6 Tag Manager, and similar technologies) to intercept, duplicate, and re-direct Plaintiffs’ and  
7 Class Members’ Private Information to third parties like Facebook, Google, Bing, Clarity  
8 and Yahoo.

10           110. The Meta Pixel, a marketing product, is a “piece of code” that allowed  
11 Defendant to “understand the effectiveness of [their] advertising and the actions  
12 [customers] take on [their] site.”<sup>23</sup> It also allowed Defendant to optimize the delivery of  
13 ads, measure cross-device conversions, create custom advertising groups or “audiences,”  
14 learn about the use of its Website, and decrease advertising and marketing costs.<sup>24</sup>

16           111. Most importantly, it allowed Facebook to secretly intercept customers’  
17 communications about their purchases of sensitive healthcare products, including fertility  
18 test kits, to diagnose and/or treat highly sensitive and private conditions on the Website.

19           ***B. Facebook’s Platform & its Business Tools.***

20           112. Facebook operates the world’s largest social media company and generated  
21 \$117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising  
22 space.<sup>25</sup>

25 <sup>23</sup> <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>  
(last visited Aug. 14, 2024).

26 <sup>24</sup> *Id.*

27 <sup>25</sup> META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS,  
[https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-  
28 Quarter-and-Full-Year-2021-Results/default.aspx](https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx), INVESTOR.FB.COM (last visited Aug. 14,  
2024).

1 113. In conjunction with its advertising business, Facebook encourages and  
 2 promotes entities and website owners, such as Defendant, to utilize its “Business Tools” to  
 3 gather, identify, target and market products and services to individuals.

4 114. Facebook’s Business Tools, including the Pixels, are bits of code that  
 5 advertisers can integrate into their webpages, mobile applications, and servers, thereby  
 6 enabling the interception and collection of user activity on those platforms.  
 7

8 115. The Business Tools are automatically configured to capture “Standard  
 9 Events” such as when a user visits a particular webpage, that webpage’s Universal Resource  
 10 Locator (“URL”), metadata, button clicks, and other user interactions with a webpage.<sup>26</sup>

11 116. Advertisers, such as Defendant, can track other user actions and can create  
 12 their own tracking parameters by building a “custom event.”<sup>27</sup>

13 117. One such Business Tool is the tracking Meta Pixel which “tracks the people  
 14 and type of actions they take.”<sup>28</sup>  
 15  
 16  
 17  
 18  
 19

20 <sup>26</sup>*Specifications for Facebook Pixel Standard Events*,  
 21 <https://www.facebook.com/business/help/402791146561655?id=1205376682832142> (last  
 21 visited Aug. 14, 2024); *see* META PIXEL, GUIDES, ADVANCED,  
 22 <https://developers.facebook.com/docs/meta-pixel/advanced> (last visited Aug. 14, 2024);  
 23 *see also* BEST PRACTICES FOR META PIXEL SETUP,  
 24 <https://www.facebook.com/business/help/218844828315224?id=1205376682832142> (last  
 24 visited Aug. 14, 2024); META MARKETING API, APP EVENTS API,  
 25 <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited Aug. 14,  
 26 2024).

27 <sup>27</sup> ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,  
 28 <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; *see*  
 26 *also* META MARKETING API, APP EVENTS API,  
 27 <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited Aug. 14,  
 28 2024).

<sup>28</sup> RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited Aug.  
 14, 2024).

1           118. When a user accesses a webpage that is hosting the Pixels, their  
2 communications with the host webpage are instantaneously and surreptitiously duplicated  
3 and sent to Facebook’s servers—traveling directly from the user’s browser to Facebook’s  
4 server.

5           119. This second, contemporaneous, and secret transmission contains the  
6 original GET request sent to the host website, along with additional data that the Pixels are  
7 configured to collect. This transmission is initiated by Facebook code and concurrent with  
8 the communications with the host website. Two sets of code are thus automatically run as  
9 part of the browser’s attempt to load and read Defendant’s Website—Defendant’s own  
10 code, and Facebook’s embedded code.

11           120. Accordingly, during the same transmissions, the Website routinely provides  
12 Facebook with its customers’ Facebook IDs, IP addresses, and/or device IDs and the other  
13 information they input into Defendant’s Website, including not only their medical searches,  
14 treatment requests, and the webpages they view, but also their name, email address, and  
15 phone number.  
16

17           121. This is precisely the type of identifying information that HIPAA requires  
18 healthcare providers to de-anonymize to protect the privacy of patients.<sup>29</sup> Plaintiffs’ and  
19 Class Members’ identities can be easily determined based on the Facebook ID, IP address  
20 and/or reverse lookup from the collection of other identifying information that was  
21 improperly disclosed.  
22  
23  
24  
25

---

26  
27 <sup>29</sup> *Guidance Regarding Methods for De-identification of Protected Health Information in*  
28 *Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy*  
*Rule*, <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Aug. 14, 2024).

1 122. After intercepting and collecting this information, Facebook processes it,  
2 analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If  
3 the website visitor is also a Facebook user, the information collected via the Facebook pixel  
4 is associated with the user's Facebook ID that identifies their name and Facebook profile,  
5 i.e., their real-world identity.

6 123. A user's FID is linked to their Facebook profile, which generally contains a  
7 wide range of demographic and other information about the user, including pictures,  
8 personal interests, work history, relationship status, and other details. Because the user's  
9 Facebook ID uniquely identifies an individual's Facebook account, Facebook—or any  
10 ordinary person—can easily use the Facebook Profile ID to quickly and easily locate,  
11 access, and view the user's corresponding Facebook profile. To find the Facebook account  
12 associated with a c\_user cookie, one simply needs to type www.facebook.com/ followed by  
13 the c\_user ID.  
14

15 124. This disclosed PHI and PII allows Facebook to know that a specific  
16 customer is seeking confidential medical care and the type of medical care being sought (in  
17 this case, purchasing sensitive healthcare products including fertility test kits used to  
18 diagnose and/or treat highly sensitive and private conditions), and Facebook then sells that  
19 information to marketers who will online target Plaintiffs and Class Members.  
20

#### 21 **IV. DEFENDANT'S USE OF THE PIXELS VIOLATES HIPAA.**

22 125. The disclosure of Plaintiffs' and Class Members' Private Information via  
23 the Pixels contravenes the letter and spirit of HIPAA's "Standards for Privacy of  
24 Individually Identifiable Health Information" (also known as the "Privacy Rule") which  
25 governs how health care providers must safeguard and protect Private Information.<sup>30</sup>  
26

27  
28 <sup>30</sup> *The HIPAA Privacy Rule*, <https://www.hhs.gov/hipaa/for->

1           126. The HIPAA Privacy Rule sets forth policies to protect all Individually  
 2 Identifiable Health Information (“IIHI”) that is held or transmitted by a covered entity such  
 3 as Defendant. These are the 18 HIPAA Identifiers that are considered personally  
 4 identifiable information because this information can be used to identify, contact, or locate  
 5 a specific person or can be used with other sources (such as a person’s Facebook account)  
 6 to identify a single individual. When IIHI is used in conjunction with one’s physical or  
 7 mental health or condition, health care, and/or one’s payment for that health care, it becomes  
 8 PHI.<sup>31</sup>

10           127. Simply put, further to the HIPAA Privacy Rule, covered entities such as  
 11 Defendant are simply *not* permitted to use tracking technology tools (like pixels) in a way  
 12 that exposes customers’ Private Information to any third party without express and informed  
 13 consent.

15           128. Under Federal Law, a healthcare provider may not disclose personally  
 16 identifiable, non-public medical information about a patient, a potential patient, or  
 17 household member of a patient for marketing purposes without the patients’ express written  
 18 authorization.<sup>32</sup>

22 [professionals/privacy/index.html](#) (last visited Aug. 14, 2024).

23 <sup>31</sup> *Guidance regarding Methods for De-identification of Protected Health Information in*  
 24 *Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy*  
 25 *Rule,* [https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html)  
 26 [identification/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html) (HIPAA Identifiers include name; address (all geographic  
 27 subdivisions smaller than state, including street address, city county, and zip code); all  
 28 elements (except years) of dates related to an individual (including birthdate, admission  
 date, discharge date, date of death, and exact age); telephone numbers; email address;  
 medical record number; health plan beneficiary number; account number; device identifiers  
 and serial numbers; web URL; internet protocol (IP) address; and any other characteristic  
 that could uniquely identify the individual) (last visited Aug. 14, 2024).

<sup>32</sup> HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

1 129. Guidance from the United States Department of Health and Human Services  
2 instructs healthcare providers that patient status alone is protected by HIPAA.

3 130. The Privacy Rule broadly defines PHI as IHI that is “transmitted by  
4 electronic media; maintained in electronic media; or transmitted or maintained in any other  
5 form or medium.” 45 C.F.R. § 160.103.

6 131. Here, Defendant provided patient information to third parties in violation of  
7 the Privacy Rule. HHS has repeatedly instructed for years that patient status is protected  
8 by the HIPAA Privacy Rule:  
9

10 a. “The sale of a patient list to a marketing firm” is not permitted  
11 under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

12 b. “A covered entity must have the individual’s prior written  
13 authorization to use or disclose protected health information for  
14 marketing communications,” which includes disclosure of mere  
15 patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14,  
16 2002); and

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

20 **V. DEFENDANT DISCLOSED PLAINTIFFS’ & CLASS MEMBERS’  
21 PRIVATE INFORMATION TO META, GOOGLE & OTHER  
22 UNAUTHORIZED THIRD PARTIES & USED PLAINTIFFS’ & CLASS  
23 MEMBERS’ PRIVATE INFORMATION FOR ITS OWN PURPOSES.**

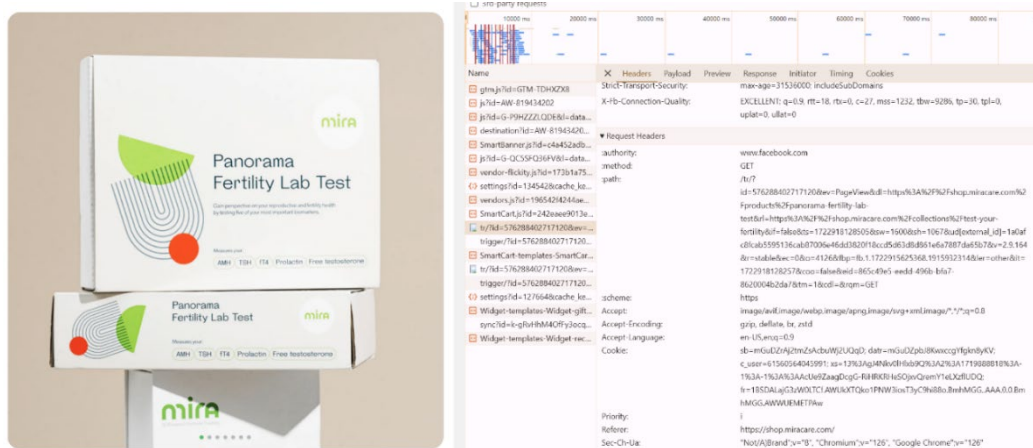
24 132. Starting on a date unknown and continuing to the present, Defendant  
25 embedded the Meta Pixel on and throughout its Website and transmitted Private  
26 Information shared by Plaintiffs and Class Members, without their consent, to Meta in  
27 accordance with the Meta Pixel’s configuration.

28 133. Defendant installed the Meta Pixel on its Website -  
https://www.miracare.com/. When Plaintiffs or another Class Member visited that website  
and completed the steps necessary to purchase sensitive healthcare products and/or test kits,



1 the Meta Pixel automatically caused the Plaintiffs' or Class Member's personal identifiers,  
 2 including IP addresses and the c\_user, \_fr, \_datr, and \_fbp cookies, to be transmitted to  
 3 Meta, attached to the fact that the Plaintiffs or Class Member had visited the Website, the  
 4 titles of the webpages the Plaintiffs or Class Member visited, and the products they  
 5 purchased.

6 **Figures 1 & 2: Examples of a HTTP single communication session sent from the**  
 7 **customer's device to Facebook that reveals the fact that the customer is searching for**  
 8 **fertility lab test and the customer's unique personal identifiers including the FID (c\_user**  
 9 **field)<sup>33</sup>:**



```

▼ Request Headers
:authority: www.facebook.com
:method: GET
:path: /tr/?
      id=576288402717120&ev=PageView&dl=https%3A%2F%2Fshop.miracare.com%2
      Fproducts%2Fpanorama-fertility-lab-
      test&rl=https%3A%2F%2Fshop.miracare.com%2Fcollections%2Ftest-your-
      fertility&if=false&ts=1722918128505&sw=1600&sh=1067&ud[external_id]=1a0af
      c8fcab5595136cab87006e46dd3820f18ccd5d63d8d861e6a7887da65b7&v=2.9.164
      &r=stable&ec=0&o=4126&fbp=fb.1.1722915625368.1915932314&ler=other&it=
      1722918128257&coo=false&eid=865c49e5-eedd-496b-bfa7-
      8620004b2da7&tm=1&cddl=&rqm=GET
:scheme: https
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
Cookie: sb=mGuDZrAj2tmZsAcbuWj2UQqD; datr=mGuDZpbJ8KwccgYfgkn8yKV;
      c_user=61560564045991; xs=13%3AgJ4Nkv0IHxb9Q%3A2%3A1719888818%3A-
    
```

<sup>33</sup> The user's Facebook ID is represented as the c\_user ID highlighted in the image below.

1           112.     The first line of Source code text, “id: 576288402717120” refers to  
2 Defendant’s Pixel ID and confirms that Defendant has downloaded the Facebook Pixel into  
3 their Source Code for this webpage.

4           113.     The second line of text, “ev: PageView,” identifies and categorizes which  
5 actions the user took on the webpage (“ev=” is an abbreviation for event, and “PageView”  
6 is the type of event). Thus, this identifies the user as viewing the page where the User can  
7 purchase the fertility lab test.  
8

9           114.     The additional lines of highlighted text show Defendant has disclosed to  
10 Facebook that the user is interested in a particular product for testing for fertility.

11           115.     Finally, the ‘method’ lines of Source code text in the images above (“GET”)  
12 demonstrate that Defendant’s Pixel sent the user’s communications, and the Private  
13 Information contained therein, alongside the user’s Facebook ID (c\_user ID), thereby  
14 allowing the user’s communications and actions on the website to be linked to their specific  
15 Facebook profile.  
16

17           116.     Rather than merely transmit the “automatic events” that the Meta Pixel  
18 automatically collects and transmits from a website without the website owner or developer  
19 being required to add any additional code, on information and belief, Defendant  
20 intentionally configured the Meta Pixel on its Website to track, collect, and disclose  
21 “custom events” such as the name of the sensitive healthcare products and/or test kits to  
22 diagnose and/or treat highly sensitive and private conditions that a customer was seeking to  
23 purchase, and the fact that the customer was purchasing these sensitive healthcare products.  
24

25           117.     To make matters worse, Defendant’s Facebook Pixel also shared with  
26 Facebook its’ customers purchasing activities, including when a User adds the product to  
27 their virtual shopping cart.  
28

1 *Figures 3 & 4: Examples of HTTP communication sessions sent from the customer's*  
 2 *device to Facebook that reveal the fact that the customer is purchasing a fertility lab test,*  
 3 *via "ViewContent" and "AddToCart" events:*

```

  4 X Headers Payload Preview Response Initiator Timing Cookies
  5 ▼Query String Parameters view source view URL-encoded
  6 id: 576288402717120
  7 ev: ViewContent
  8 dl: https://shop.miracare.com/products/panorama-fertility-lab-test
  9 rl: https://shop.miracare.com/collections/test-your-fertility
  10 if: false
  11 ts: 1722918128784
  12 cd[content_name]: Mira Panorama Fertility Lab Test
  13 cd[contents]: [{"id":"8980165689637","name":"Mira Panorama Fertility Lab Test","content_categor
  14 y":"","item_price":"179.00"}]
  15 cd[content_category]:
  16 cd[content_ids]: 8980165689637
  17 cd[content_type]: product_group
  18 cd[value]: 179.00
  19 cd[currency]: USD
  
```

```

  20 X Headers Payload Preview Response Initiator Timing Cookies
  21 ▼Query String Parameters view source view URL-encoded
  22 id: 576288402717120
  23 ev: AddToCart
  24 dl: https://shop.miracare.com/products/panorama-fertility-lab-test
  25 rl: https://shop.miracare.com/collections/test-your-fertility
  26 if: false
  27 ts: 1722918487001
  28 cd[content_ids]: 8980165689637
  29 cd[contents]: [{"id":"8980165689637","name":"Mira Panorama Fertility Lab Test","content_categor
  30 y":"","item_price":"179.00","quantity":"1"}]
  31 cd[content_name]: Mira Panorama Fertility Lab Test
  32 cd[content_type]: product_group
  33 cd[value]: 179.00
  34 cd[content_category]:
  35 cd[currency]: USD
  
```

118. In each of the examples above, the user's website activity and the contents  
 of the user's communications are sent to Facebook alongside their personally identifiable  
 information. Several different methods allow marketers and third parties to identify  
 individual website users, but the examples above demonstrate what happens when the  
 website user is logged into Facebook on their web browser or device. When this happens,  
 the website user's identity is revealed via third-party cookies that work in conjunction with  
 the Pixel. For example, the Pixel transmits the user's c\_user cookie, which contains that

1 user's unencrypted Facebook ID, and allows Facebook to link the user's online  
2 communications and interactions to their individual Facebook profile.

3 119. Facebook receives at least five cookies when Defendant's Website  
4 transmits information via the Pixel, including the c\_user, datr, and fr cookies:

5

6

7

8

9

10

11



Name	Value	Domain	Path	Exp...	Size
c_user	615605...	.facebook.com	/	202...	20
datr	mGuD...	.facebook.com	/	202...	28
fr	1BSDA...	.facebook.com	/	202...	82
sb	mGuD...	.facebook.com	/	202...	26
xs	13%3A...	.facebook.com	/	202...	96

12 120. The "datr" cookie contains a unique alphanumeric code and identifies the  
13 specific web browser from which the user is sending the communication. It is an identifier  
14 that is unique to the user's web browser and is therefore a means of identification for Meta.  
15 Meta keeps a record of every datr cookie identifier associated with each of its users.  
16

17 121. The fr cookie, a unique combination of the c\_user and datr cookies,  
18 contains an encrypted Facebook ID and browser identifier.<sup>34</sup> Facebook, at a minimum, uses  
19 the fr cookie to identify users, and this particular cookie can stay on a user's website browser  
20 for up to 90 days after the user has logged out of Facebook.<sup>35</sup>  
21

22 122. The datr and fr cookies are commonly referred to as third-party cookies  
23 because they were "created by a website with a domain name other than the one the user is  
24

25

26 <sup>34</sup> Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit*, p. 33 (Sept.  
27 21, 2012), [http://www.europe-v-facebook.org/ODPC\\_Review.pdf](http://www.europe-v-facebook.org/ODPC_Review.pdf) (last visited July 20,  
28 2024).

<sup>35</sup> *Cookies & other storage technologies*, <https://www.facebook.com/policy/cookies/> (last  
visited July 20, 2024).

1 currently visiting”—i.e., Facebook. Although Facebook created these cookies, Defendant  
 2 is ultimately responsible for the manner in which individual website users were identified  
 3 via these cookies, and Facebook would not have received this data but for Defendant’s  
 4 implementation and use of the Pixel throughout the Website.

5 123. Defendant also revealed the Website visitors’ identities via first-party  
 6 cookies such as the `_fbp` cookie that Facebook uses to identify a particular browser and a  
 7 User:

Name	Value	Domain	Path	Exp...	Size	Http...	Sec...	Sa...
<code>_fbp</code>	fb.1.17...	.miracare.com	/	202...	33			Lax

11 124. The `fbp` cookie is a Facebook identifier that is set by Facebook source code  
 12 and associated with Defendant’s use of the Facebook Meta Pixel program. The `fbp` cookie  
 13 emanates from Defendant’s Website as a putative first party cookie, but is transmitted to  
 14 Facebook through cookie synching technology that hacks around the same-origin policy.  
 15 Therefore, the `_fbp` cookie is transmitted to Facebook even when the user’s browser is  
 16 configured to block third-party tracking cookies.

18 125. The `__ga` and `_gid` cookies operate similarly as to Google.

Name	Value	Domain	Path	Exp...	Size	Http...	Sec...	Sa...	Part...
<code>_ga</code>	GA1.1....	.miracare.com	/	202...	30				
<code>_ga_P9HZZZLQDE</code>	GS1.1.1...	.miracare.com	/	202...	51				
<code>_ga_QC5SFQ36FV</code>	GS1.1.1...	.miracare.com	/	202...	52				

22 126. The Facebook Pixel uses both first- and third-party cookies to link website  
 23 visitors’ communications and online activity with their corresponding Facebook profiles,  
 24 and, because the Pixel is automatically programmed to transmit data via both first-party and  
 25 third-party cookies, customers’ information and identities are revealed to Facebook even  
 26 when they have disabled third-party cookies within their web browsers.

1           127. At present, the full breadth of Defendant's tracking and data sharing  
2 practices is unclear, but other evidence suggests Defendant has been using additional  
3 Tracking Tools to transmit their users' Private Information to additional third parties. For  
4 example, Plaintiffs' counsels' investigation revealed that Defendant was also sending their  
5 customers' protected health information to Google via Google tracking tools including  
6 Google Analytics and Google Tag Manager.

7  
8           128. Defendant does not disclose that the Pixel, Google trackers, first-party  
9 cookies from third parties like Facebook and/or Google, or any other Tracking Tools  
10 embedded in the Website's source code track, record, and transmit Plaintiffs' and Class  
11 Members' Private Information to Facebook and Google for targeted advertising. Moreover,  
12 Defendant never received consent or written authorization to disclose Plaintiffs' and Class  
13 Members' private communications to Facebook or Google for marketing.

14  
15           129. Thus, put simply, when Plaintiffs or other Class Members used Defendant's  
16 website to purchase fertility test kits, their identities, personal identifiers, and health  
17 information (including their medical conditions and treatments sought) were disclosed to  
18 Meta.

19           130. On information and belief, Defendant disclosed Plaintiffs' and Class  
20 Members' Private Information to Meta in order to permit Defendant to improve its  
21 marketing and advertising and increase its revenues and profits.

22  
23 **VI. DEFENDANT DOES NOT DISCLOSE THAT IT SENDS PRIVATE**  
24 **INFORMATION TO THIRD PARTIES FOR MARKETING PURPOSES AND,**  
**AS SUCH, VIOLATES ITS OWN PRIVACY POLICIES.**

25           131. Defendant breached Plaintiffs' and Class Members' right to privacy by  
26 unlawfully disclosing their Private Information to the Pixel Information Recipients.  
27 Specifically, Plaintiffs had a reasonable expectation of privacy based on Defendant's own  
28

1 representations to Plaintiffs and the Class that Defendant would not disclose their Private  
2 Information to third parties.

3 132. Defendant's privacy policies, despite their increasing breadth over the years  
4 with respect to sharing customers' data, have never specifically disclosed to Plaintiffs or  
5 Class Members that their viewing or purchase of sensitive healthcare products, including  
6 fertility testing kits, and other Private Information will be disclosed to third parties; nor has  
7 Defendant ever obtained informed consent from Plaintiffs or Class Members to do so.<sup>36</sup>

9 133. In the Privacy Policy in effect at the time of Plaintiffs' purchase, Defendant  
10 did not inform Plaintiffs that they shared their Private Information with Facebook or the  
11 other Pixel Information Recipients.<sup>37</sup> In fact, prior to a revision implemented on March 8,  
12 2024, Defendant's Privacy Policy expressly stated, "Mira shall not retain, use or disclose  
13 any personal information provided by Customer except as necessary for the specific purpose  
14 of provision of Mira's products and services for Customer."<sup>38</sup>

16 134. Defendant breached Plaintiffs' and Class Members' right to privacy by  
17 unlawfully disclosing their Private Information to the Pixel Information Recipients.  
18 Specifically, Plaintiffs and Class Members had a reasonable expectation of privacy (based  
19 on Defendant's own representations to Plaintiffs and the Class).

20 135. Specifically, Defendant did not inform Plaintiffs that it was sharing her  
21 Private Information with Facebook and the other Pixel Information Recipients. Moreover,  
22 Defendant's Privacy Policy did not state that user and customer Private Information will be  
23 shared with Facebook or other unauthorized third parties.  
24

25  
26 <sup>36</sup> <https://www.miracare.com/privacy-policy/> (implemented in March 2024).

27 <sup>37</sup> [https://web.archive.org/web/20210122162958/https://www.miracare.com/privacy-](https://web.archive.org/web/20210122162958/https://www.miracare.com/privacy-policy/)  
[policy/](https://web.archive.org/web/20210122162958/https://www.miracare.com/privacy-policy/) (implemented July 3, 2018).

28 <sup>38</sup> [https://web.archive.org/web/20230609064724/https://www.miracare.com/privacy-](https://web.archive.org/web/20230609064724/https://www.miracare.com/privacy-policy/)  
[policy/](https://web.archive.org/web/20230609064724/https://www.miracare.com/privacy-policy/) (implemented December 16, 2022).

1 136. By engaging in this improper sharing of information without Plaintiffs' and  
2 Class Members' consent, Defendant violated its own Privacy Policy and breached  
3 Plaintiffs' and Class Members' right to privacy and unlawfully disclosed their Private  
4 Information.

5 **VII. USERS' REASONABLE EXPECTATION OF PRIVACY.**

6 137. Plaintiffs and Class Members were aware of Defendant's duty of  
7 confidentiality when they sought sensitive healthcare supplies from Defendant.  
8

9 138. Indeed, at all times when Plaintiffs and Class Members provided their PII  
10 and PHI to Defendant, they each had a reasonable expectation that the information would  
11 remain confidential and that Defendant would not share the Private Information with third  
12 parties for a commercial purpose unrelated to patient care.

13 139. Privacy polls and studies show that the overwhelming majority of  
14 Americans consider obtaining an individual's affirmative consent before a company  
15 collects and shares that individual's data to be one of the most important privacy rights.  
16

17 140. For example, a recent Consumer Reports study shows that 92% of  
18 Americans believe that internet companies and websites should be required to obtain  
19 consent before selling or sharing consumer data, and the same percentage believe those  
20 companies and websites should be required to provide consumers with a complete list of  
21 the data that is collected about them.<sup>39</sup>  
22

23 141. Personal data privacy and obtaining consent to share Private Information  
24 were material to Plaintiffs and Class Members in their purchases of Defendant's test kits.

25 \_\_\_\_\_  
26 <sup>39</sup> *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey*  
27 *Findings*, (May 11, 2017), [https://www.consumerreports.org/consumer-reports/consumers-](https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/)  
28 [less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/](https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/) (last visited  
Aug. 14, 2024).



1 **VIII. DEFENDANT WAS ENRICHED & BENEFITTED FROM THE USE OF**  
2 **THE PIXELS & UNAUTHORIZED DISCLOSURES.**

3 142. The primary motivation and a determining factor in Defendant's  
4 interception and disclosure of Plaintiffs' and Class Members' Private Information was to  
5 commit criminal and tortious acts in violation of federal and state laws as alleged herein,  
6 namely, the use of customer data for advertising in the absence of express written consent.  
7 Defendant's further use of the Private Information after the initial interception and  
8 disclosure for marketing and revenue generation was in violation of HIPAA and an invasion  
9 of privacy.

10 143. Defendant used the Pixels on its Website for its own purposes of marketing  
11 and profits.

12 144. Based on information and belief, Defendant receives compensation from  
13 third parties like Facebook and Google in the form of enhanced advertising services and  
14 more cost-efficient marketing on third-party platforms in exchange for disclosing  
15 customers' personally identifiable information.

16 145. Based on information and belief, Defendant was advertising its services on  
17 Facebook, for one, and the Pixels were used to "help [Mira] understand which types of ads  
18 and platforms are getting the most engagement[.]"<sup>40</sup>

19 146. Retargeting is a form of online marketing that targets users with ads based  
20 on their previous Internet communications and interactions.

21 147. Upon information and belief, Defendant re-targeted customers and potential  
22 customers to get more people to use its services and purchase its products. These customers  
23 include Plaintiffs and Class Members.  
24  
25  
26

27  
28 <sup>40</sup> RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited Aug. 14, 2024).

1 148. By utilizing the Pixels, Defendant's cost of advertising and retargeting was  
2 reduced, thereby benefitting and enriching Defendant.

3 **IX. PLAINTIFFS' & CLASS MEMBERS' DATA HAS FINANCIAL VALUE.**

4 149. Moreover, Plaintiffs' and Class Members' Private Information had value  
5 and Defendant's interception and unauthorized disclosure thereof harmed Plaintiffs and the  
6 Class.

7  
8 150. Conservative estimates suggest that in 2018, Internet companies earned  
9 \$202 per American user from mining and selling data. That figure is only due to keep  
10 increasing; estimates for 2022 are as high as \$434 per user, for a total of more than \$200  
11 billion industry wide.

12 151. The value of health data in particular is well-known and has been reported  
13 on extensively in the media. For example, Time Magazine published an article in 2017 titled  
14 "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it  
15 described the extensive market for health data and observed that the market for information  
16 was both lucrative and a significant risk to privacy.<sup>41</sup>

17  
18 152. Similarly, CNBC published an article in 2019 in which it observed that  
19 "[d]e-identified patient data has become its own small economy: There's a whole market of  
20 brokers who compile the data from providers and other health-care organizations and sell it  
21 to buyers."<sup>42</sup>

22  
23 153. Several companies have products through which they pay consumers for a  
24 license to track certain information. Google, Nielsen, UpVoice, HoneyGain, and  
25 SavvyConnect are all companies that pay for browsing history information.

26  
27 <sup>41</sup> See <https://time.com/4588104/medical-data-industry/> (last visited Aug. 14, 2024).

28 <sup>42</sup> See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited Aug. 14, 2024).

1           154. Facebook itself has paid users for their digital information, including  
2 browsing history. Until 2019, Facebook ran a “Facebook Research” app through which it  
3 paid \$20 a month for a license to collect browsing history information and other  
4 communications from consumers between the ages 13 and 35.

5           155. Tech companies are under particular scrutiny because they already have  
6 access to a massive trove of information about people, which they use to serve their own  
7 purposes, including potentially micro-targeting advertisements to people with certain health  
8 conditions.  
9

10           156. Policymakers are proactively calling for a revision and potential upgrade of  
11 the HIPAA privacy rules out of concern for what might happen as tech companies continue  
12 to march into the medical sector.<sup>43</sup>

13           157. The Private Information at issue here is also a valuable commodity to  
14 identity thieves. As the FTC recognizes, identity thieves can use Private Information to  
15 commit an array of crimes that include identity theft and medical and financial fraud.<sup>44</sup> A  
16 robust “cyber black market” exists where criminals openly post stolen PII and PHI on  
17 multiple underground Internet websites, commonly referred to as the dark web.  
18

19           158. While credit card information and associated IHHI can sell for as little as  
20 \$1–\$2 on the black market, PHI can sell for as much as \$363.<sup>45</sup>

21           159. PHI is particularly valuable because criminals can use it to target victims  
22 with frauds that take advantage of their medical conditions.  
23  
24

---

25 <sup>43</sup> *Id.*

26 <sup>44</sup> FTC, *Warning Signs of Identity Theft*, [https://www.consumer.ftc.gov/articles/0271-  
warning-signs-identity-theft](https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft) (last visited Aug. 14, 2024).

27 <sup>45</sup> Center for Internet Security, *Data Breaches: In the Healthcare Sector*,  
28 <https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/> (last accessed June  
24, 2024).

1           160.    PHI can also be used to create fraudulent insurance claims and facilitate the  
2 purchase and resale of medical equipment, and it can help criminals gain access to  
3 prescriptions for illegal use or sale.

4           161.    Medical identity theft can result in inaccuracies in medical records, costly  
5 false claims, and life-threatening consequences. If a victim's health information is  
6 comingled with other records, it can lead to misdiagnoses or mistreatment.

7  
8           162.    The FBI Cyber Division issued a Private Industry Notification on April 8,  
9 2014 that advised the following:

10           Cyber criminals are selling [medical] information on the black  
11 market at a rate of \$50 for each partial EHR, compared to \$1 for a  
12 stolen social security number or credit card number. EHR can then  
13 be used to file fraudulent insurance claims, obtain prescription  
14 medication, and advance identity theft. EHR theft is also more  
15 difficult to detect, taking almost twice as long as normal identity  
16 theft.

17           163.    Cybercriminals often trade stolen Private Information on the black market  
18 for years following a breach or disclosure. Stolen Private Information can be posted on the  
19 Internet, making it publicly available.

20           164.    Defendant gave away Plaintiffs' and Class Members' communications and  
21 transactions on its Website without permission.

22           165.    The unauthorized access to Plaintiffs' and Class Members' Private  
23 Information has diminished the value of that information, resulting in harm to Users,  
24 including Plaintiffs and Class Members.

25           **X.    DEFENDANT USED AND DISCLOSED PLAINTIFFS' & CLASS**  
26           **MEMBERS' PRIVATE INFORMATION WITHOUT PLAINTIFFS' OR**  
27           **CLASS MEMBERS' KNOWLEDGE, CONSENT, AUTHORIZATION OR**  
28           **FURTHER ACTION.**

          166.    The tracking tools incorporated into, embedded in, or otherwise permitted  
on Defendant's Website were invisible to Plaintiffs and Class Members while using that

1 Website. The Meta Pixels on Defendant's Website were seamlessly integrated into the  
2 Website such that there was no reason for Plaintiffs or any Class Member to be aware of or  
3 to discover their presence.

4 167. Plaintiffs and Class Members were shown no disclaimer or warning that  
5 their Private Information would be disclosed to any unauthorized third party without their  
6 express consent.

7  
8 168. Plaintiffs and Class Members had no idea that their Private Information was  
9 being collected and transmitted to an unauthorized third party.

10 169. Because Plaintiffs and Class Members had no idea of the presence of Meta  
11 Pixels on Defendant's Website, or that their Private Information would be collected and  
12 transmitted to Meta, they could not and did not consent to Defendant's conduct.

13 170. Plaintiffs and Class Members did not give consent or authorization for  
14 Defendant to disclose their Private Information to Meta or to any third party for marketing  
15 purposes.

16  
17 171. Moreover, Defendant's Notice of Privacy Practices, as described above,  
18 provided no indication to Plaintiffs or Class Members that their Private Information would  
19 be disclosed to Meta or any unauthorized third party.

20 **TOLLING, CONCEALMENT & ESTOPPEL**

21 172. Any applicable statutes of limitation have been tolled by Defendant's  
22 knowing and active concealment of its incorporation of the Meta Pixel into its website.

23  
24 173. The Meta Pixel and other tracking tools on Defendant's website were and  
25 are entirely invisible to a website visitor.

26 174. Through no fault or lack of diligence, Plaintiffs and Class Members were  
27 deceived and could not reasonably discover Defendant's deception and unlawful conduct.  
28

1 175. Plaintiffs were ignorant of the information essential to pursue their claims,  
2 without any fault or lack of diligence on her part.

3 176. Defendant had exclusive knowledge that its Website incorporated the Meta  
4 Pixel and other tracking tools and yet failed to disclose to customers, including Plaintiffs  
5 and Class Members, that by purchasing sensitive healthcare products and/or test kits,  
6 Plaintiffs' and Class Members' Private Information would be disclosed or released to Meta  
7 and other unauthorized third parties.  
8

9 177. Under the circumstances, Defendant was under a duty to disclose the nature,  
10 significance, and consequences of its collection and treatment of its customers' Private  
11 Information. In fact, to the present Defendant has not conceded, acknowledged, or  
12 otherwise indicated to its customers that it has disclosed or released their Private  
13 Information to unauthorized third parties. Accordingly, Defendant is estopped from relying  
14 on any statute of limitations.  
15

16 178. Moreover, all applicable statutes of limitation have also been tolled  
17 pursuant to the discovery rule.

18 179. The earliest that Plaintiffs or Class Members, acting with due diligence,  
19 could have reasonably discovered Defendant's conduct would have been shortly before the  
20 filing of this Complaint.

21 180. Plaintiff Mora first discovered that Defendant had collected and shared her  
22 Private Information without her consent on or around June 2024 after contacting  
23 undersigned counsel and discussing potential claims against Defendant. For Plaintiff  
24 Moreno, this discovery occurred in early August 2024.  
25

26  
27 **CLASS ALLEGATIONS**  
28

1 181. This action is brought by the named Plaintiffs on their behalf and on behalf  
2 of a proposed Class of all other persons similarly situated under Federal Rules of Civil  
3 Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

4 182. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

5  
6 **The Nationwide Class**

7 All natural persons who used Defendant's Website to purchase human  
8 healthcare products to treat sensitive health conditions whose Private  
9 Information was disclosed or transmitted to Meta or any other unauthorized  
third party.

10 183. In addition to the claims asserted on behalf of the Nationwide Class,  
11 Plaintiff Frances Mora asserts claims on behalf of the Florida Subclass and Plaintiff Moreno  
12 asserts claims on behalf of the California Subclass, which are defined as follows:

13  
14 **The Florida Subclass**

15 All natural persons residing in Florida who used Defendant's Website to  
16 purchase human healthcare products to treat sensitive health conditions  
17 whose Private Information was disclosed or transmitted to Meta or any other  
unauthorized third party.

18  
19 **The California Subclass**

20 All natural persons residing in California who used Defendant's Website to  
21 purchase human healthcare products to treat sensitive health conditions  
whose Private Information was disclosed or transmitted to Meta or any other  
unauthorized third party.

22 184. Excluded from the proposed Class are any claims for personal injury,  
23 wrongful death, or other property damage sustained by the Class; and any Judge conducting  
24 any proceeding in this action and members of their immediate families.

25 185. Plaintiffs reserve the right to amend the definitions of the Class or add  
26 subclasses if further information and discovery indicate that the definitions of the Class  
27 should be narrowed, expanded, or otherwise modified.  
28

1           186.    **Numerosity.** The Class is so numerous that the individual joinder of all  
2 members is impracticable. Upon information and belief, there are tens of thousands of Mira  
3 customers that have been impacted by Defendant’s actions. Moreover, the exact number of  
4 those impacted is generally ascertainable by appropriate discovery and is in the exclusive  
5 control of Defendant.

6           187.    **Commonality.** Common questions of law or fact arising from Defendant’s  
7 conduct exist as to all members of the Class, which predominate over any questions  
8 affecting only individual Class Members. These common questions include, but are not  
9 limited to, the following:  
10

- 11           a)       Whether and to what extent Defendant had a duty to protect the  
12                   Private Information of Plaintiffs and Class Members;
- 13           b)       Whether Defendant had duties not to disclose the Private  
14                   Information of Plaintiffs and Class Members to unauthorized  
15                   third parties;
- 16           c)       Whether Defendant violated its own privacy policy by  
17                   disclosing the Private Information of Plaintiffs and Class  
18                   Members to the Pixel Information Recipients;
- 19           d)       Whether Defendant adequately, promptly, and accurately  
20                   informed Plaintiffs and Class Members that their Private  
21                   Information would be disclosed to third parties;
- 22           e)       Whether Defendant violated the law by failing to promptly  
23                   notify Plaintiffs and Class Members that their Private  
24                   Information was being disclosed without their consent;
- 25           f)       Whether Defendant adequately addressed and fixed the practices  
26                   which permitted the unauthorized disclosure of customers’  
27                   Private Information;
- 28           g)       Whether Defendant engaged in unfair, unlawful, or deceptive  
                 practices by failing to keep the Private Information belonging to  
                 Plaintiffs and Class Members free from unauthorized disclosure;



- 1 h) Whether Defendant violated the statutes asserted as claims in  
2 this Complaint;
- 3 i) Whether Plaintiffs and Class Members are entitled to actual,  
4 consequential, and/or nominal damages as a result of  
5 Defendant's wrongful conduct;
- 6 j) Whether Defendant knowingly made false representations as to  
7 its data security and/or privacy policy practices;
- 8 k) Whether Defendant knowingly omitted material representations  
9 with respect to its data security and/or privacy policy practices;  
10 and
- 11 l) Whether Plaintiffs and Class Members are entitled to injunctive  
12 relief to redress the imminent and currently ongoing harm faced  
13 as a result of the Defendant's disclosure of their Private  
14 Information.

15 188. **Typicality.** Plaintiffs' claims are typical of those of other Class Members  
16 because Plaintiffs' Private Information, like that of every other Class Member, was  
17 compromised as a result of Defendant's incorporation and use of the Pixels and/or  
18 Conversions API.

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

26 190. **Predominance.** Defendant has engaged in a common course of conduct  
27 toward Plaintiffs and Class Members in that all the Plaintiffs' and Class Members' data was  
28 unlawfully stored and disclosed to unauthorized third parties, including the Pixel

1 Information Recipients, in the same way. The common issues arising from Defendant's  
2 conduct affecting Class Members set out above predominate over any individualized issues.  
3 Adjudication of these common issues in a single action has important and desirable  
4 advantages of judicial economy.

5         191. **Superiority.** A class action is superior to other available methods for the  
6 fair and efficient adjudication of the controversy. Class treatment of common questions of  
7 law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class  
8 action, most Class Members would likely find that the cost of litigating their individual  
9 claim is prohibitively high and would therefore have no effective remedy. The prosecution  
10 of separate actions by individual Class Members would create a risk of inconsistent or  
11 varying adjudications with respect to individual Class Members, which would establish  
12 incompatible standards of conduct for Defendant. In contrast, the conduct of this action as  
13 a class action presents far fewer management difficulties, conserves judicial resources and  
14 the parties' resources, and protects the rights of each Class member.

15  
16  
17         192. Defendant has acted on grounds that apply generally to the Class as a whole  
18 so that class certification, injunctive relief, and corresponding declaratory relief are  
19 appropriate on a class-wide basis.

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

- 24  
25         a) Whether Defendant owed a legal duty to Plaintiffs and the Class to  
26 exercise due care in collecting, storing, and safeguarding their Private  
27 Information and not disclosing it to unauthorized third parties;  
28

- 1 b) Whether Defendant breached a legal duty to Plaintiffs and Class  
2 Members to exercise due care in collecting, storing, using, and  
3 safeguarding their Private Information;
- 4 c) Whether Defendant failed to comply with its own policies and  
5 applicable laws, regulations, and industry standards relating to data  
6 security;
- 7 d) Whether Defendant adequately and accurately informed Plaintiffs and  
8 Class Members that their Private Information would be disclosed to  
9 third parties;
- 10 e) Whether Defendant failed to implement and maintain reasonable  
11 security procedures and practices appropriate to the nature and scope of  
12 the information disclosed to third parties;
- 13 f) Whether Class Members are entitled to actual, consequential, and/or  
14 nominal damages and/or injunctive relief as a result of Defendant's  
15 wrongful conduct.

16 194. Finally, all members of the proposed Class are readily ascertainable.  
17 Defendant has access to Class Members' names and addresses affected by the unauthorized  
18 disclosures that have taken place. Class Members have already been preliminarily identified  
19 and sent Notice by Defendant.

20 **COUNT I**  
21 **VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT**  
22 **18 U.S.C. § 2511(1), *et seq.***  
23 **Unauthorized Interception, Use, and Disclosure**  
24 ***(On Behalf of Plaintiffs & the Nationwide Class)***

25 195. Plaintiffs re-allege and incorporate by reference the allegations above as if  
26 fully set forth herein.

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

197. The ECPA protects both sent and received communications.

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

4           199. The interception and transmission of Plaintiffs’ and Class Members’ Private  
5 Information via Defendant’s Website is a “communication” under the ECPA’s definition  
6 under 18 U.S.C. § 2510(12).

7  
8           200. The transmission of Private Information between Plaintiffs and Class  
9 Members and Defendant via the Website are “transfer[s] of signs, signals, writing, ... data,  
10 [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio,  
11 electromagnetic, photoelectronic, or photooptical system that affects interstate commerce”  
12 and are therefore “electronic communications” within the meaning of 18 U.S.C. § 2510(2).

13           201. The ECPA defines “content” when used with respect to electronic  
14 communications to “include[] any information concerning the substance, purport, or  
15 meaning of that communication.” 18 U.S.C. § 2510(8).

16  
17           202. The ECPA defines “interception” as the “acquisition of the contents of any  
18 wire, electronic, or oral communication through the use of any electronic, mechanical, or  
19 other device” and “contents ... include any information concerning the substance, purport,  
20 or meaning of that communication.” 18 U.S.C. § 2510(4), (8).

21           203. The ECPA defines “electronic, or other device” as “any device ... which  
22 can be used to intercept a[n] ... electronic communication[.]” 18 U.S.C. § 2510(5).

23  
24           204. The following constitute “devices” within the meaning of 18 U.S.C. §  
25 2510(5):

- 26           a. The cookies Defendant and Facebook use to track Plaintiffs’ and Class  
27 Members’ communications;

- 1           b. Plaintiffs' and Class Members' browsers;
- 2           c. Plaintiffs' and Class Members' computing devices;
- 3           d. Defendant's web servers; and
- 4           e. The Pixels deployed by Defendant to effectuate the sending and acquisition of
- 5           user and patient sensitive communications.

6           205. By utilizing and embedding the Pixels on the Website and/or servers,

7

8 Defendant intentionally intercepted, endeavored to intercept, and procured another person

9 to intercept, the electronic communications of Plaintiffs and Class Members, in violation of

10 18 U.S.C. § 2511(1)(a).

11           206. Specifically, Defendant intercepted Plaintiffs' and Class Members'

12 electronic communications via the Pixels, which tracked, stored, and unlawfully disclosed

13 Plaintiffs' and Class Members' Private Information to Facebook.

14           207. Whenever Plaintiffs and Class Members interacted with Defendant's

15 Website, Defendant, through the Pixel and other tracking technologies it embedded and

16 operated on the Website, contemporaneously and intentionally redirected and disclosed the

17 contents of Plaintiffs' and Class Members' electronic communications while those

18 communications were in transmission, to persons or entities other than an addressee or

19 intended recipient of such communication, including Facebook.

20           208. Defendant intercepted communications that included, but are not limited to,

21

22 communications to/from Plaintiffs and Class Members regarding IIHI and PHI, including

23 IP address, Facebook ID, and health information relevant to the screenings and testing,

24 which Plaintiffs and Class Members sought to purchase.

25           209. Additionally, through the above-described Pixel and other tracking

26 technologies, Defendant intercepted communications, this information was, in turn, used

27

28

1 by third parties, such as Facebook, to 1) place Plaintiffs in specific health-related categories  
2 based on their past, present and future health conditions and 2) target Plaintiffs with  
3 particular advertising associated with her specific health conditions.

4 210. By intentionally disclosing or endeavoring to disclose the electronic  
5 communications of Plaintiffs and Class Members to the Pixel Information Recipients and,  
6 potentially, other third parties, while knowing or having reason to know that the information  
7 was obtained through the interception of an electronic communication in violation of 18  
8 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

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

15 212. Defendant intentionally intercepted the contents of Plaintiffs' and Class  
16 Members' electronic communications for the purpose of committing a tortious act in  
17 violation of the Constitution or laws of the United States or of any State—namely, invasion  
18 of privacy, among others.

19 213. Defendant intentionally used the wire or electronic communications to  
20 increase its profit margins. Defendant specifically used the Pixels to track and utilize  
21 Plaintiffs' and Class Members' Private Information for its own financial benefit.

23 214. Defendant was not acting under color of law to intercept Plaintiffs' and  
24 Class Members' wire or electronic communications.

25 215. Plaintiffs and Class Members did not authorize Defendant to acquire the  
26 content of their communications for purposes of invading Plaintiffs' and Class Members'  
27 privacy via the Pixels.  
28

1           216. Any purported consent that Defendant received from Plaintiffs and Class  
2 Members was not valid.

3           217. In sending and in acquiring the content of Plaintiffs' and Class Members'  
4 communications relating to the browsing of Defendant's Website, creation of accounts,  
5 participation in Defendant's health screenings, and/or purchasing a subscription plan,  
6 Defendant's purpose was tortious and designed to violate federal and state law, including  
7 as described above, a knowing intrusion into a private place, conversation, or matter that  
8 would be highly offensive to a reasonable person.  
9

10           218. The party exception in § 2511(2)(d) does not permit a party that intercepts  
11 or causes interception to escape liability if the communication is intercepted for the purpose  
12 of committing any tortious or criminal act in violation of the Constitution or laws of the  
13 United States or of any State.

14           219. Because of Defendant's simultaneous, unknown duplication, forwarding  
15 and interception of Plaintiffs' and Class Members' Private Information, Defendant does not  
16 qualify for the party exemption.  
17

18           220. Here, as alleged above, Defendant violated a provision of HIPAA,  
19 specifically 42 U.S.C. § 1320d-6(a)(3), which imposes a criminal penalty for knowingly  
20 disclosing IIHI to a third party.  
21

22           221. HIPAA defines IIHI as:

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

1           222. Plaintiffs’ information that Defendant disclosed to third parties qualifies as  
2 IIHI, and Defendant violated Plaintiffs’ expectations of privacy, and constitutes tortious  
3 and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant used the  
4 wire or electronic communications to increase their profit margins. Defendant specifically  
5 used the Pixel to intercept and then disclose Plaintiffs’ and Class Members’ Private  
6 Information for financial gain.

7  
8           223. The penalty for a violation of HIPAA is enhanced where “the offense is  
9 committed with intent to sell, transfer, or use IIHI for commercial advantage, personal gain,  
10 or malicious harm.” 42 U.S.C. § 1320d-6.

11           224. Defendant’s conduct violated 42 U.S.C. § 1320d-6 in that it: (i) used and  
12 caused to be used cookie identifiers associated with specific customers without customer  
13 authorization; and (ii) disclosed IIHI to Facebook and other third parties without customer  
14 authorization.

15  
16           225. Defendant’s conduct would be subject to the enhanced provisions of 42  
17 U.S.C. § 1320d-6 because Defendant’s use of the Facebook source code was for  
18 Defendant’s commercial advantage to increase revenue from existing customers and gain  
19 new customers.

20           226. Healthcare customers have the right to rely upon the promises that  
21 companies make to them. Defendant accomplished its tracking and retargeting through  
22 deceit and disregard, such that an actionable claim may be made, in that it was accomplished  
23 through source code that cause Facebook Pixels and other tracking codes (including but not  
24 limited to the fbp, ga and gid cookies) and other tracking technologies to be deposited on  
25 Plaintiffs’ and Class members’ computing devices as “first-party” cookies that are not  
26 blocked.  
27  
28



1 227. Defendant knew or had reason to know that the fbp, ga, and gid cookies  
2 would command Plaintiffs' and Class Members' computing devices to remove, redirect,  
3 and disclose their data and the content of their communications with Defendant to Facebook  
4 and others.

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

11 **COUNT II**  
12 **NEGLIGENCE**  
13 ***(On Behalf of Plaintiffs & the Nationwide Class)***

14 229. Plaintiffs re-allege and incorporate by reference the allegations above as if  
15 fully set forth herein.

16 230. Defendant required Plaintiffs and Class Members to submit non-public  
17 personal information in order to obtain healthcare/medical services.

18 231. By collecting and storing this data in Defendant's computer systems,  
19 Defendant had a duty of care to use reasonable means to secure and safeguard its computer  
20 systems—and Class Members' Private Information held within it—to prevent disclosure of  
21 the information, and to safeguard the information from disclosure to third parties.

22 232. Defendant owed a duty of care to Plaintiffs and Class Members to provide  
23 data security consistent with industry standards, the statements it made in its Privacy Policy,  
24 and other requirements discussed herein, and to ensure that its systems and networks, and  
25 the personnel responsible for them, adequately protected the Private Information.  
26  
27  
28

1           233. Defendant’s duty of care to use reasonable security measures arose as a  
2 result of the special relationship that existed between Defendant and its customers, which  
3 is recognized by laws and regulations including but not limited to HIPAA, the FTC Act,  
4 state privacy statutes, as well as common law.

5           234. Defendant was in a position to ensure that its systems were sufficient to  
6 protect against the foreseeable risk of harm to Class Members from a Data Breach.

7           235. Defendant’s duty to use reasonable security measures under HIPAA  
8 required Defendant to “reasonably protect” confidential data from “any intentional or  
9 unintentional use or disclosure” and to “have in place appropriate administrative, technical,  
10 and physical safeguards to protect the privacy of protected health information.” 45 C.F.R.  
11 § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue  
12 in this case constitutes “protected health information” within the meaning of HIPAA.  
13

14           236. In addition, Defendant had a duty to employ reasonable security measures  
15 under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits  
16 “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by  
17 the FTC, the unfair practice of failing to use reasonable measures to protect confidential  
18 data.  
19

20           237. Defendant’s duty to use reasonable care in protecting confidential data arose  
21 not only as a result of the statutes and regulations described above, but also because  
22 Defendant is bound by industry standards to protect confidential Private Information.  
23

24           238. Defendant also had a duty to protect Plaintiffs’ and Class Members’ Private  
25 Information from disclosure consistent with the representations it made in its Privacy  
26 Policy.  
27  
28

1           239. Plaintiffs and Class Members had reasonable expectations of privacy in  
2 their communications exchanged with Defendant, including communications exchanged on  
3 Defendant's Website.

4           240. Contrary to its duties as a medical provider and its express promises of  
5 confidentiality, Defendant installed its Tracking Tools to disclose and transmit to third  
6 parties Plaintiffs' and Class Members' communications with Defendant, including Private  
7 Information and the contents of such information.  
8

9           241. These disclosures were made without Plaintiffs' or Class Members'  
10 knowledge, consent, or authorization, and were unprivileged.

11           242. The third-party recipients included, but may not be limited to, Facebook  
12 and/or Google.

13           243. As a direct and proximate cause of Defendant's unauthorized disclosures of  
14 patient personally identifiable, non-public medical information, and communications,  
15 Plaintiff and Class members were damaged by Defendant's breach in that:  
16

- 17           a. Sensitive and confidential information that Plaintiffs and  
18           Class members intended to remain private is no longer  
19           private;
- 20           b. Plaintiffs and Class members face ongoing harassment and  
21           embarrassment in the form of unwanted targeted  
22           advertisements;
- 23           c. Defendant eroded the essential confidential nature of the  
24           provider-patient relationship;
- 25           d. General damages for invasion of their rights in an amount  
26           to be determined by a jury;
- 27           e. Nominal damages for each independent violation;
- 28           f. Defendant took something of value from Plaintiffs and  
            Class Members and derived benefit therefrom without  
            Plaintiffs' and Class Members' knowledge or informed  
            consent and without compensation for such data;

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- g. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant’s duty to maintain confidentiality;
- h. Defendant’s actions diminished the value of Plaintiffs’ and Class Members’ Private Information; and
- i. Defendant’s actions violated the property rights Plaintiffs and Class Members have in their Private Information.

244. It was foreseeable that Defendant’s failure to use reasonable measures to protect Plaintiffs’ and Class Members’ Private Information would result in injury to Plaintiffs and Class Members.

245. Plaintiffs and Class Members are entitled to compensatory, nominal, and/or punitive damages.

**COUNT III**  
**VIOLATIONS OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. §§ 501.201, et seq.**  
***(On Behalf of Plaintiff Mora & the Florida Subclass)***

246. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

247. Defendant engaged in unfair and unlawful acts and trade practices by failing to maintain adequate procedures to avoid disclosure of Plaintiff Mora’s and Florida Subclass Members’ Private Information and permitting access to this Private Information by the Pixel Information Recipients.

248. Plaintiff Mora and Florida Subclass members relied on Defendant’s implied promise of data privacy and security when providing their Private Information to Defendant.

249. The Florida Deceptive and Unfair Trade Practices Act (“FDUTPA”), codified in Fla. Stat. §§ 501.201 – 501.213, prohibits unfair and deceptive trade practices

1 in the course of any business or occupation.

2 250. Plaintiff has a private right action pursuant to NRS 41.600(2)(e).

3 251. By reason of the conduct alleged herein, Defendant knowingly engaged in  
4 unlawful trade practices within the meaning of the FDUTPA. Defendant's conduct alleged  
5 herein falls within the FDUTPA's definition for "trade or commerce," and the deception  
6 occurred within the State of Florida.

7  
8 252. Plaintiff Mora and other members of the Florida Subclass used Defendant's  
9 Website from Florida. Their Private Information was collected and transmitted by operation  
10 of the Pixels and other tracking codes, which were instantiated in the Source Code running  
11 in their browser or mobile application.

12 253. Defendant solicited, obtained, and stored Plaintiff Mora's and Florida  
13 Subclass Members' Private Information and knew or should have known not to disclose  
14 such Private Information to the Pixel Information Recipients through use of the Pixels and  
15 other tracking technologies.

16  
17 254. Plaintiff Mora and Florida Subclass Members would not have provided their  
18 Private Information if they had been told or knew that Defendant would be disclosing such  
19 information to the Pixel Information Recipients and others.

20 255. Defendant's conduct violated Fla. Stat. § 501.204 because it constituted  
21 "[u]nfair methods of competition, unconscionable acts [and] practices, and unfair or  
22 deceptive acts or practices in the conduct of [] trade or commerce," *i.e.*,:

- 23  
24 a. Representing that its services were of a particular standard or quality that it  
25 knew or should have known were of another;
- 26 b. Failing to implement and maintain reasonable security and privacy measures to  
27 protect Plaintiff Mora's and Florida Subclass Members' Private Information  
28 from unauthorized disclosure;

- 1 c. Failing to comply with common law and statutory duties pertaining to the  
2 security and privacy of Plaintiff Mora’s and Florida Subclass Members’ Private  
3 Information, including duties imposed by Section 5 of the FTCA, 15 U.S.C. §  
4 45, which prohibits “unfair . . . practices in or affecting commerce,” including,  
5 as interpreted and enforced by the FTC, the unfair practice of failing to use  
6 reasonable measures to protect confidential data, and HIPAA. Defendant’s  
7 failure was a direct and proximate cause of the unauthorized disclosure of  
8 Plaintiff Mora’s and Florida Subclass Members’ Private Information;
- 9 d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff  
10 Mora’s and Florida Subclass Members’ Private Information from unauthorized  
11 disclosure;
- 12 e. Omitting, suppressing, and concealing the material fact that it did not intend to  
13 protect Plaintiff Mora’s and Florida Subclass Members’ Private Information  
14 from unauthorized disclosure, and
- 15 f. Omitting, suppressing, and concealing the material fact that it did not comply  
16 with common law and statutory duties pertaining to the security and privacy of  
17 Plaintiff Mora’s and Florida Subclass Members’ Personal Information,  
18 including duties imposed by the FTCA and HIPAA, which failure was a direct  
19 and proximate cause of the unauthorized disclosure.

20 256. Defendant’s representations and omissions were material because they were  
21 likely to deceive reasonable consumers about the adequacy of Defendant’s data security  
22 and ability to protect the confidentiality of consumers’ Private Information.

23 257. Such acts by Defendant are and were deceptive trade practices which are  
24 and/or were likely to mislead a reasonable consumer by providing his or her Private  
25 Information to Defendant.

26 258. Defendant knew or should have known that its computer systems and data  
27 security practices—in particular, their use of the Pixels and Conversions API—were  
28 inadequate to safeguard the Private Information of Plaintiff Mora and Florida Subclass  
Members, and that enabling third parties to collect the Private Information of Plaintiff and  
the Florida Subclass constituted a data breach.

29 259. Defendant’s violations of the FDUTPA have an impact and general

1 importance to the public, including the people of Florida. Upon information and belief,  
2 thousands of Florida citizens have had their Private Information transmitted without consent  
3 from Defendant's Website to third parties.

4 260. As a direct and proximate result of these deceptive trade practices, Plaintiff  
5 Mora and Florida Subclass Members have suffered injuries including, but not limited to  
6 actual damages, and in being denied a benefit conferred on them by the Florida legislature.  
7

8 261. Accordingly, Plaintiff Mora, on behalf of herself and Florida Subclass  
9 Members, brings this action under the FDUTPA, to seek such injunctive relief necessary to  
10 enjoin further violations, to recover actual damages, treble damages, the costs of this action  
11 (including reasonable attorneys' fees and costs), and such other relief as the Court deems  
12 just and proper.

13  
14 **COUNT IV**  
15 **VIOLATION OF FLORIDA SECURITY OF COMMUNICATIONS ACT**  
16 **("FSCA") Fla. Stat. § 934.01 *et seq.***  
17 ***(On Behalf of Plaintiff Mora and the Florida Subclass)***

18 262. Plaintiffs re-allege and incorporate by reference the allegations above as if  
19 fully set forth herein.

20 263. Where there is a reasonable expectation of privacy, absent the consent of all  
21 parties, the FSCA prohibits, among other things, the intentional interception or procurement  
22 of another person to intercept any wire, oral or electronic communication. Fla. Stat. §§  
23 934.03(1), 934.03(2)(d).

24 264. The FSCA prohibits: (1) the interception or procurement of another to  
25 intercept any wire, oral or electronic communication; (2) the intentional disclosure of the  
26 contents of any wire, oral or electronic communication that the discloser knew or should  
27 have known was obtained through the interception of a wire, oral or electronic  
28 communication; and (3) the intentional use of the contents of any wire, oral or electronic

1 communication that the discloser knew or should have known was obtained through the  
2 interception of a wire, oral or electronic communication. Fla. Stat. 934.03(1).

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

9  
10       266. Under the FSCA, "wire communication" means "any aural transfer made in  
11 whole or in part through the use of facilities for the transmission of communications by the  
12 aid of wire, cable, or other like connection between the point of origin and the point of  
13 reception including the use of such connection in a switching station furnished or operated  
14 by any person engaged in providing or operating such facilities for the transmission of  
15 intrastate, interstate, or foreign communications or communications affecting intrastate,  
16 interstate, or foreign commerce." Fla. Stat. § 934.02(1).

17  
18       267. Under the FSCA, "intercept" is defined as the "[a]ural or other acquisition  
19 of the contents of any wire, electronic, or oral communication through the use of any  
20 electronic, mechanical, or other device." Fla. Stat. § 934.02(3).

21  
22       268. Under the FSCA, "contents" in the context of "any wire, oral, or electronic  
23 communication, includes any information concerning the substance, purport, or meaning of  
24 that communication." Fla. Stat. § 934.02(7).

25       269. Under the FSCA, "person" is defined as "any individual, partnership,  
26 association, joint stock company, trust, or corporation." Fla. Stat. § 934.02(5).



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

6           271. By utilizing and embedding the Pixel on its Web Properties, Defendant  
7 intentionally intercepted, endeavored to intercept, and procured another person to intercept,  
8 the electronic communications of Plaintiff and Florida Subclass Members  
9 contemporaneously including communications regarding the selection of doctors, locations  
10 of medical care, specific searches provided by Plaintiff and Florida Subclass Members for  
11 medical conditions, diagnosis and treatment—while navigating the Web Properties.

12           272. Defendant contemporaneously intercepted these communications without  
13 authorization and consent from Plaintiff and Florida Subclass Members.  
14

15           273. Defendant intercepted Plaintiff’s and Florida Subclass Members’  
16 communications to contemporaneously learn the meaning of the content of Plaintiff’s and  
17 Florida Subclass Members’ communications.  
18

19           274. Plaintiff and Florida Subclass Members had a justified and reasonable  
20 expectation under the circumstances that their electronic communications would not be  
21 intercepted.  
22

23           275. Plaintiff and Florida Subclass Members were not aware that their electronic  
24 communications were being intercepted by Facebook and did not consent to the  
25 interception.  
26  
27  
28



1           284.    This claim is pleaded in the alternative to Plaintiffs’ other causes of action.

2           285.    Defendant benefits from the use of Plaintiffs’ and Class Members’ Private  
3 Information and unjustly retained those benefits at Plaintiffs’ and Class Members’ expense.

4           286.    Plaintiffs and Class Members conferred a benefit upon Defendant in the  
5 form of the monetizable Private Information that Defendant collected from them and  
6 disclosed to third parties, including the Pixel Information Recipients, without authorization  
7 and proper compensation.  
8

9           287.    Additionally, Plaintiffs conferred a benefit upon Defendant when they  
10 signed up for accounts with Defendant and purchased prescriptions through Defendant.

11           288.    Defendant consciously collected and used this information for their own  
12 gain, providing Defendant with economic, intangible, and other benefits, including  
13 substantial monetary compensation.  
14

15           289.    Defendant unjustly retained those benefits at the expense of Plaintiffs and  
16 Class Members because Defendant conduct damaged Plaintiffs and Class Members, all  
17 without providing any commensurate compensation to Plaintiffs or Class Members.

18           290.    The benefits that Defendant derived from Plaintiffs and Class Members  
19 were not offered by Plaintiffs or Class Members gratuitously and, thus, rightly belongs to  
20 Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles  
21 for Defendant to be permitted to retain any of the profit or other benefits wrongly derived  
22 from the unfair and unconscionable methods, acts, and trade practices alleged in this  
23 Complaint.  
24

25           291.    Had Defendant informed Plaintiffs that it collected and shared Plaintiffs’  
26 Private Information with the Pixel Information Recipients, Plaintiffs would have refused to  
27 consent to such use of her Private Information or would have demanded compensation for  
28

1 such usage. Now knowing of Defendant’s practices, Plaintiffs demands compensation for  
2 the unauthorized use of her Private Information.

3 292. Defendant should be compelled to disgorge into a common fund for the  
4 benefit of Plaintiffs and the Class all unlawful or inequitable proceeds that Defendant  
5 received, and such other relief as the Court may deem just and proper.

6  
7 **COUNT VI**  
8 **VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (“CIPA”),**  
9 **Cal. Penal Code § 631**  
10 ***(On Behalf of Plaintiff Moreno, the California Subclass, & the Nationwide Class)***

11 293. Plaintiffs re-allege and incorporate by reference the allegations above as if  
12 fully set forth herein.

13 294. CIPA § 631(a) imposes liability for “distinct and mutually independent  
14 patterns of conduct.” *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to  
15 establish liability under CIPA § 631(a), a Plaintiffs need only establish that the defendant,  
16 “by means of any machine, instrument, contrivance, or in any other manner,” does any of  
17 the following:

18 Intentionally taps, or makes any unauthorized connection, whether  
19 physically, electrically, acoustically, inductively or otherwise, with  
20 any telegraph or telephone wire, line, cable, or instrument, including  
21 the wire, line, cable, or instrument of any internal telephonic  
22 communication system,

23 Or

24 Willfully and without the consent of all parties to the  
25 communication, or in any unauthorized manner, reads or attempts to  
26 read or learn the contents or meaning of any message, report, or  
27 communication while the same is in transit or passing over any wire,  
28 line or cable or is being sent from or received at any place within  
this state,

Or

Uses, or attempts to use, in any manner, or for any purpose, or to  
communicate in any way, any information so obtained,

Or

Aids, agrees with, employs, or conspires with any person or persons

1 to unlawfully do, or permit, or cause to be done any of the acts or  
2 things mentioned above in this section.

3 295. Section 631(a) is not limited to phone lines, but also applies to “new  
4 technologies” such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016  
5 WL 8200619, at \*21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and  
6 must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley*  
7 *v. Google, Inc.*, 2006 WL 3798134, at \*5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs  
8 “electronic communications”); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d  
9 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on  
10 Facebook’s collection of consumers’ Internet browsing history).

11 296. The Pixels are a “machine, instrument, contrivance, or ... other manner”  
12 used to engage in the prohibited conduct at issue here.

13 297. At all relevant times, by employing the Pixels, Defendant intentionally  
14 tapped, electrically or otherwise, the lines of internet communication between Plaintiffs and  
15 Class Members on the one hand, and Defendant’s Website on the other hand.

16 298. At all relevant times, Defendant aided, agreed with, employed, and  
17 conspired with the Pixel Information Recipients to use the Pixels to wiretap consumers to  
18 Defendant’s Website and to accomplish the wrongful conduct at issue here.

19 299. The wrongful conduct at issue occurred in the State of California, where  
20 Defendant maintain their principal place of business.

21 300. Plaintiffs and Class Members did not consent to the Pixel Information  
22 Recipients’ intentional access, interception, reading, learning, recording, and collection of  
23 Plaintiffs’ and Class Members’ electronic communications. Nor did Plaintiffs and Class  
24 Members consent to Defendant aiding, agreeing with, employing, or otherwise enabling the  
25 Pixel Information Recipients’ conduct.  
26  
27  
28



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**DEMAND FOR JURY TRIAL**

Plaintiffs, on behalf of themselves and other members of the proposed Classes,  
hereby demand a jury trial on all issues so triable.

Dated: August 16, 2024

Respectfully submitted,

**ALMEIDA LAW GROUP LLC**

By: /s/ Matthew J. Langley  
Matthew J. Langley (SBN 342286)  
849 W. Webster Avenue  
Chicago, Illinois 60614  
Tel: (773) 554-9354  
Email: matt@almeidawgroup.com

David DiSabato\*  
Tyler Bean\*  
**SIRI & GLIMSTAD LLP**  
8 Campus Drive, Suite 105, PMB#161  
Parsippany, New Jersey 07054  
Tel: (212) 532-1091  
[ddisabato@sirillp.com](mailto:ddisabato@sirillp.com)  
[tbean@sirillp.com](mailto:tbean@sirillp.com)

*\*pro hac vice admission anticipated*  
  
*Attorneys for Plaintiffs & the Classes*

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Fertility Test Kit Provider Mira Secretly Shares Consumers' Private Data with Advertisers, Class Action Lawsuit Alleges](#)

---