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

Attorneys for Plaintiffs & the Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

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

Plaintiffs,

v.

QUANOVATE TECH INC. d/b/a MIRA,

Defendant

Case No.

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

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

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

NATURE OF THE ACTION

1. Defendant is a self-proclaimed "mini hormone lab" that offers both male and female customers at-home fertility testing and monitoring using quantitative technology.[1]

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

3. Information concerning a person's physical and mental health is among the most confidential and sensitive information in our society and the mishandling of such information can have serious consequences including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.[2]

---

[1] *See* https://www.miracare.com/how-mira-works/ (last visited Aug. 14, 2024).

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

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

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

---

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

[3] *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-information-bakers-dozen-takeaways-ftc-cases (last visited Aug. 14, 2024).

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

> **Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.**
>
> In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.***
>
> [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that ***may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information***.[4]

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

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

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

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

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

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

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

12. That investigation found that "trackers collecting browsing- and purchase-related data on websites on 12 of the biggest drugstores in the United States, including grocery store chains with pharmacies, and sharing the sensitive information with companies like Meta and Google, through their advertising and analytics products and Microsoft, through its search engine, Bing."[8]

---

[5] *See, e.g., Top Mental Health & Prayer Apps Fail Spectacularly at Privacy, Security* (May 2, 2022), https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security/ (last visited Aug. 14, 2024).

[6] As noted by the FTC, at-home test kit providers should be upfront with customers about what data they collect, how it is stored and with whom it is shared.

[7] *See* Danielle Ellis, *Need to get Plan B or an HIV test online? Facebook may know about 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).

[8] *Id.*

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

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

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

16. Defendant's unlawful privacy violations occurred and continue to occur because of the tracking technologies that it installed on its website including, but not limited to, the Meta Pixel, Google Analytics, Google DoubleClick and Google Tag Manager (collectively, "Tracking Tools").[11]

---

[9] *See, supra,* n.2. Moreover, the policies of many test providers fail to include specific limitations around data retention and deletion, instead relying on vague, catchall language.

[10] Kaylana Mueller-Hsia & Laura Hecht-Fellala, *Evaluating the Privacy of At-Home Covid 19 Tests, The Tests Are Essential for Fighting the Pandemic, but Poor Privacy Policy Practices Could Discourage Some People from Using Them*, BRENNAN CENTER FOR 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).

[11] While this Complaint focuses on tracking tools from Facebook and Google, research

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

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

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

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

---

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

[12] Regardless, Facebook tracks and collects data even on people who don't have a Facebook account or have deactivated their Facebook accounts. They can be in an even worse 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."

21. They also send cookies – a way of storing information in a user's browser that helps track a user from page to page as the user browses a retailer's site.[13]

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

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

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

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

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

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

[13] Cookies are often also used to associate individuals on a site with their account on a social media platform, such as Facebook or Instagram.

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

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

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

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

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

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

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

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

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

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

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

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

[14] *See* Defendant's *Privacy Policy*, https://www.miracare.com/privacy-policy/.

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

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

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

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

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

[15] Molly Osberg & Dhruv Mehrotral, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137 (last visited Aug. 14, 2024); *see also* Timothy M. Hale, PhD & Joseph C. Kvedar, MD, *Privacy and Security Concerns in Telehealth* (Dec. 2014), 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).

> publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… ***If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.*** [16]

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

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

---

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

[17] *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 (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.

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

43. Despite incorporating the Pixels, Conversions API, and other third-party tracking technologies into its Website and servers, Mira has never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook.[18]

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

[18] 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; *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies* (Oct. 20, 2022),

44. As a result of Mira's conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lack of trust in communicating with health providers online; (iii) emotional distress and heightened concerns related to the release of Private Information to third parties, (iv) loss of benefit of the bargain; (v) diminution of value of their Private Information; (vi) statutory damages and (viii) continued and ongoing risk to their Private Information.

45. Plaintiffs therefore seek on behalf of themselves and a class of similarly situated persons, to remedy these harms and therefore assert the following statutory and common law claims against Mira: (i) Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq*., Unauthorized Interception, Use and Disclosure; (ii) Negligence; (iii) Florida's Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, *et seq*.; (iv) Violation of Florida Security of Communications Act, Fla. Stat. § 934.01 *et seq.*; (v) Unjust Enrichment and (vi) Violation of the California Invasion of Privacy Act, Cal. Penal Code § 934.01 *et seq.*

PARTIES

https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3; *Novant Health Notifies 1.3M Patients of Unauthorized PHI Disclosure Caused By Meta Pixel* (Aug. 17, 2022), https://healthitsecurity.com/news/novant-health-notifies-patients-of-unauthorized-phi-disclosure-caused-by-meta-pixel (last visited Aug. 14, 2024).

46. Plaintiff Carla Moreno is, and at all relevant times was, an individual residing in Paso Robles, San Luis Obispo County, in the State of California and brings this action in an individual capacity and on behalf of all others similarly situated.

47. Plaintiff Frances Mora is, and at all relevant times was, an individual residing in Miami, Miami-Dade County, in the State of Florida and brings this action in an individual capacity and on behalf of all others similarly situated.

48. Defendant Quanovate Tech Inc. d/b/a Mira is a Delaware corporation with its principal place of business located at 2010 Crow Canyon Place, San Ramon, CA 94583.

JURISDICTION & VENUE

49. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because this Complaint asserts a claim for violation of federal law, specifically, the ECPA, 18 U.S.C. § 2511. This Court has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

50. This Court also has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative Class Members, and minimal diversity exists because Plaintiffs and many putative Class Members are citizens of a different state than Defendant.

51. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in this District. Further, Defendant is authorized to and regularly conducts business in this District and makes decisions regarding corporate governance and management of the Website in this District, including decisions regarding the privacy of customers' IIHI and PHI and the incorporation of the Pixels and other tracking technologies.

52. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because: a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the unauthorized sharing of Plaintiffs' and Class Members' Private Information; Defendant's principal place of business is located in this District; Defendant collects and redistributes Class Members' Private Information in this District; and Defendant caused harm to Class Members residing in this District.

PLAINTIFFS' ALLEGATIONS

Plaintiff Moreno

53. In and around April 2022, Plaintiff Moreno utilized Defendant's Website on her personal electronic devices to research and purchase at-home fertility test kits, including those offered for sale by Defendant on its Website.

54. Specifically, Plaintiff has purchased an at-home fertility test product such as Mira Hormone Monitor: Max Kit in April 2022 from Mira's Website.

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

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

57. Plaintiff Moreno never consented to or authorized Defendant to disclose her Private Information to third parties or for Defendant to enable third parties to access, interpret and use such Private Information.

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

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

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

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

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

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

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

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

Plaintiff Mora

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FACTUAL ALLEGATIONS

I. THE USE OF TRACKING PIXELS IN THE HEALTHCARE INDUSTRY.

79. A "pixel" is a piece of code that "tracks the people and the types of actions they take"[19] as they interact with a website, including how long a person spends on a particular webpage, which buttons the person clicks, which pages they view, the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box) and much, much more.

80. When embedded on a company's website, the Pixels send data about user activity, including what you are viewing, your searches on websites, purchases you have made, items added to a shopping cart, and even information you filled out in online forms.[20] Meta calls this activity "interactions."

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

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

83. Here, a user's web browser executes the Pixels via instructions within each webpage of Defendant's Website to communicate certain information (within parameters set by Defendant) directly to the corresponding Pixel Information Recipients.

---

[19] *Retargeting*, https://www.facebook.com/business/goals/retargeting (last visited Aug. 14, 2024).

[20] *See* Tom Kemp, *"Oops! I Did It Again" ... Meta Pixel Still Hoovering Up Our Sensitive 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).

84. The Pixels can also share the user's identifying information for easy tracking via the "cookies"[21] stored on their computer by any of the Pixel Information Recipients with which they have an account.

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

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

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

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

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

[21] "Cookies are small files of information that a web server generates and sends to a web browser Cookies help inform websites about the user, enabling the websites to personalize the user experience." *See* https://www.cloudflare.com/learning/privacy/what-are-cookies/ last visited Aug. 14, 2024).

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

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

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

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

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

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

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

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

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

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.

- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.

- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data. [22]

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

97. Every website is comprised of Markup and "Source Code." Source Code is 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.

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

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

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

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

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

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

103. Defendant intentionally configured Pixels installed on its Website to capture both the "characteristics" of individual customers' communications with the

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

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

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

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

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

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

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

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

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

B. Facebook's Platform & its Business Tools.

112. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[25]

---

[23] https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Aug. 14, 2024).

[24] *Id.*

[25] META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, 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).

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

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

115. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL"), metadata, button clicks, and other user interactions with a webpage.[26]

116. Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[27]

117. One such Business Tool is the tracking Meta Pixel which "tracks the people and type of actions they take."[28]

---

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

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

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

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

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

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

121. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[29] Plaintiffs' and Class Members' identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

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

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

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

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

IV. DEFENDANT'S USE OF THE PIXELS VIOLATES HIPAA.

125. The disclosure of Plaintiffs' and Class Members' Private Information via the Pixels contravenes the letter and spirit of HIPAA's "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") which governs how health care providers must safeguard and protect Private Information.[30]

[30] *The HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-

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

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

128. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[32]

---

professionals/privacy/index.html (last visited Aug. 14, 2024).

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

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

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

130. The Privacy Rule broadly defines PHI as IIHI that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

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

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

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

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

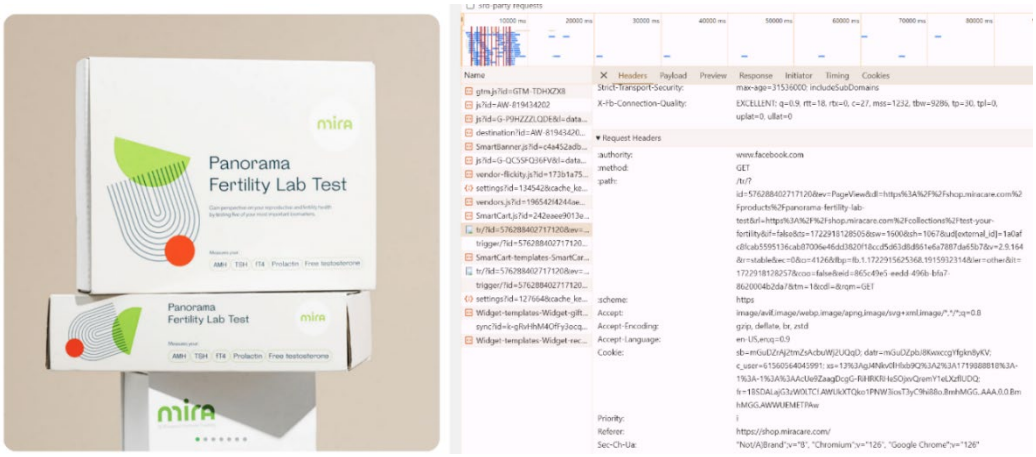
V. DEFENDANT DISCLOSED PLAINTIFFS' & CLASS MEMBERS' PRIVATE INFORMATION TO META, GOOGLE & OTHER UNAUTHORIZED THIRD PARTIES & USED PLAINTIFFS' & CLASS MEMBERS' PRIVATE INFORMATION FOR ITS OWN PURPOSES.

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

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,

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

Figures 1 & 2: Examples of a HTTP single communication session sent from the customer's device to Facebook that reveals the fact that the customer is searching for fertility lab test and the customer's unique personal identifiers including the FID (c_user field)[33]:



[33] The user's Facebook ID is represented as the c_user ID highlighted in the image below.

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

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

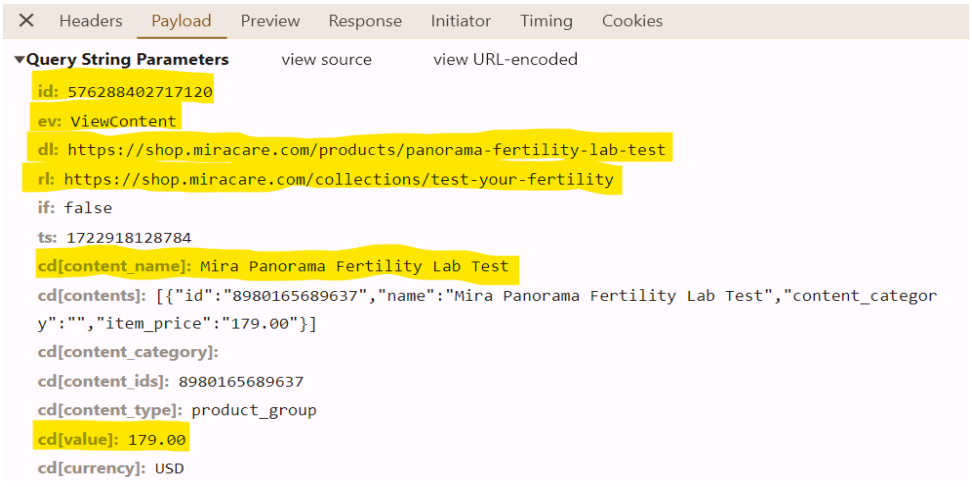
114. The additional lines of highlighted text show Defendant has disclosed to Facebook that the user is interested in a particular product for testing for fertility.

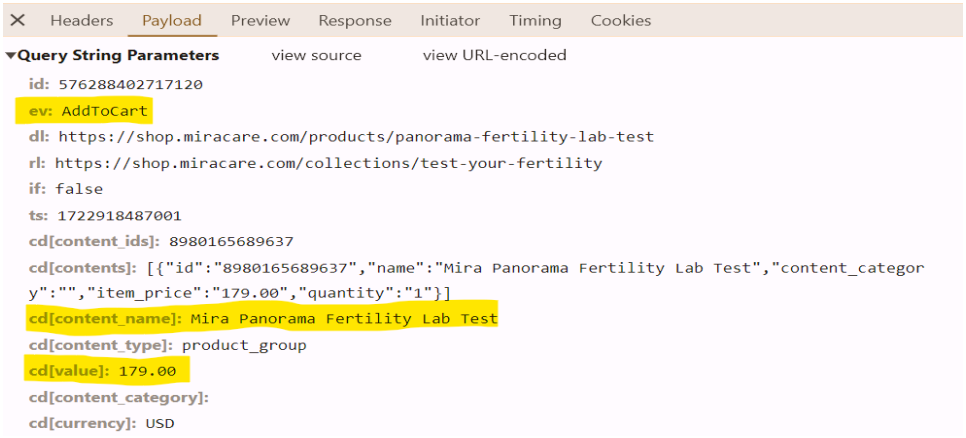
115. Finally, the 'method' lines of Source code text in the images above ("GET") demonstrate that Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the user's Facebook ID (c_user ID), thereby allowing the user's communications and actions on the website to be linked to their specific Facebook profile.

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

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

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

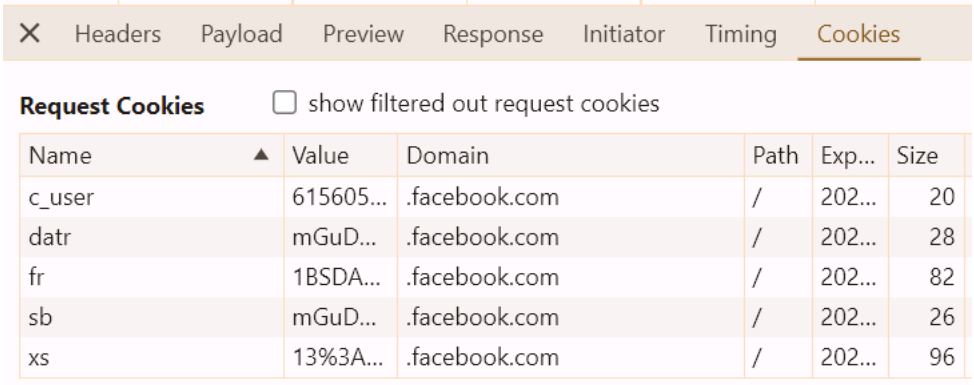




118. In each of the examples above, the user's website activity and the contents of the user's communications are sent to Facebook alongside their personally identifiable information. Several different methods allow marketers and third parties to identify individual website users, but the examples above 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

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

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



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

121. The fr cookie, a unique combination of the c_user and datr cookies, contains an encrypted Facebook ID and browser identifier.[34] Facebook, at a minimum, uses the fr cookie to identify users, and this particular cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.[35]

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

---

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

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

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

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

Name	Value	Domain	Path	Exp...	Size	Htt...	Sec...	Sa...
_fbp	fb.1.17...	.miracare.com	/	202...	33			Lax

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

[36] https://www.miracare.com/privacy-policy/ (implemented in March 2024).
[37] https://web.archive.org/web/20210122162958/https://www.miracare.com/privacy-policy/ (implemented July 3, 2018).
[38] https://web.archive.org/web/20230609064724/https://www.miracare.com/privacy-policy/ (implemented December 16, 2022).

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

VII. USERS' REASONABLE EXPECTATION OF PRIVACY.

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

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

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

140. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[39]

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

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

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

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

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

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

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

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

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

[40] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Aug. 14, 2024).

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

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

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

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

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

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

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

[41] *See* https://time.com/4588104/medical-data-industry/ (last visited Aug. 14, 2024).
[42] *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).

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

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

156. Policymakers are proactively calling for a revision and potential upgrade of the HIPAA privacy rules out of concern for what might happen as tech companies continue to march into the medical sector.[43]

157. The Private Information at issue here is also a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use Private Information to commit an array of crimes that include identity theft and medical and financial fraud.[44] A robust "cyber black market" exists where criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

158. While credit card information and associated IIHI can sell for as little as $1–$2 on the black market, PHI can sell for as much as $363.[45]

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

---

[43] *Id.*

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

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

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

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

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

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

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

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

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

X. DEFENDANT USED AND DISCLOSED PLAINTIFFS' & CLASS MEMBERS' PRIVATE INFORMATION WITHOUT PLAINTIFFS' OR CLASS MEMBERS' KNOWLEDGE, CONSENT, AUTHORIZATION OR 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

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

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

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

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

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

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

TOLLING, CONCEALMENT & ESTOPPEL

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

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

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

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

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

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

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

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

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

CLASS ALLEGATIONS

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

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

The Nationwide Class

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

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

The Florida Subclass

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

The California Subclass

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

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

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

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

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

a) Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b) Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c) Whether Defendant violated its own privacy policy by disclosing the Private Information of Plaintiffs and Class Members to the Pixel Information Recipients;

d) Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

e) Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information was being disclosed without their consent;

f) Whether Defendant adequately addressed and fixed the practices which permitted the unauthorized disclosure of customers' Private Information;

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;

h) Whether Defendant violated the statutes asserted as claims in this Complaint;

i) Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j) Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;

k) Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices; and

l) Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their Private Information.

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

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

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

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

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

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

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

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

b) Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c) Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d) Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

e) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

f) Whether Class Members are entitled to actual, consequential, and/or nominal damages and/or injunctive relief as a result of Defendant's wrongful conduct.

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

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

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

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

197. The ECPA protects both sent and received communications.

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

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

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

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

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

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

204. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The cookies Defendant and Facebook use to track Plaintiffs' and Class Members' communications;

b. Plaintiffs' and Class Members' browsers;

c. Plaintiffs' and Class Members' computing devices;

d. Defendant's web servers; and

e. The Pixels deployed by Defendant to effectuate the sending and acquisition of user and patient sensitive communications.

205. By utilizing and embedding the Pixels on the Website and/or servers, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

206. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the Pixels, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Private Information to Facebook.

207. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Pixel and other tracking technologies it embedded and operated on the Website, contemporaneously and intentionally redirected and disclosed the contents of Plaintiffs' and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook.

208. Defendant intercepted communications that included, but are not limited to, communications to/from Plaintiffs and Class Members regarding IIHI and PHI, including IP address, Facebook ID, and health information relevant to the screenings and testing, which Plaintiffs and Class Members sought to purchase.

209. Additionally, through the above-described Pixel and other tracking technologies, Defendant intercepted communications, this information was, in turn, used

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

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

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

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

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

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

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

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

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

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

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

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

221. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) **relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual,** and (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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

238. Defendant also had a duty to protect Plaintiffs' and Class Members' Private Information from disclosure consistent with the representations it made in its Privacy Policy.

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

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

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

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

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

a. Sensitive and confidential information that Plaintiffs and Class members intended to remain private is no longer private;

b. Plaintiffs and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

d. General damages for invasion of their rights in an amount to be determined by a jury;

e. Nominal damages for each independent violation;

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;

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

in the course of any business or occupation.

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

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

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

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

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

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

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Mora's and Florida Subclass Members' Private Information from unauthorized disclosure;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Mora's and Florida Subclass Members' Private Information, including duties imposed by Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data, and HIPAA. Defendant's failure was a direct and proximate cause of the unauthorized disclosure of Plaintiff Mora's and Florida Subclass Members' Private Information;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Mora's and Florida Subclass Members' Private Information from unauthorized disclosure;

e. Omitting, suppressing, and concealing the material fact that it did not intend to protect Plaintiff Mora's and Florida Subclass Members' Private Information from unauthorized disclosure, and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Mora's and Florida Subclass Members' Personal Information, including duties imposed by the FTCA and HIPAA, which failure was a direct and proximate cause of the unauthorized disclosure.

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

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

258. Defendant knew or should have known that its computer systems and data security practices—in particular, their use of the Pixels and Conversions API—were 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

273. Defendant intercepted Plaintiff's and Florida Subclass Members' communications to contemporaneously learn the meaning of the content of Plaintiff's and Florida Subclass Members' communications.

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

275. Plaintiff and Florida Subclass Members were not aware that their electronic communications were being intercepted by Facebook and did not consent to the interception.

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

277. Defendant willfully, knowingly, intentionally, and voluntarily engaged in the aforementioned acts when they incorporated the Meta Pixel on their Web Properties, with knowledge of the Pixel's purpose and functionality, and further utilized the benefits that Pixel provides website owners to the detriment of Plaintiff and the Florida Subclass Members.

278. Plaintiff and the Florida Subclass Members could not have avoided the harms described herein through the exercise of ordinary diligence.

279. As a result of Defendant's actions, Plaintiff and Florida Subclass Members have suffered harm and injury.

280. Plaintiff and Florida Subclass Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

281. Plaintiff and the Florida Subclass Members seek appropriate relief for these injuries, including but not limited to damages that will reasonably compensate them for the harm to their privacy interests as a result of Defendant's violation of the FSCA.

282. Plaintiff and Florida Subclass Members seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

COUNT V
UNJUST ENRICHMENT
(*On Behalf of Plaintiffs & the Nationwide Class*)

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

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

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

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

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

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

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

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

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

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

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

COUNT VI
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA"), Cal. Penal Code § 631
(*On Behalf of Plaintiff Moreno, the California Subclass, & the Nationwide Class*)

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

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

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> Or
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> 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

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

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

296. The Pixels are a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

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

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

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

300. Plaintiffs and Class Members did not consent to the Pixel Information Recipients' intentional access, interception, reading, learning, recording, and collection of Plaintiffs' and Class Members' electronic communications. Nor did Plaintiffs and Class Members consent to Defendant aiding, agreeing with, employing, or otherwise enabling the Pixel Information Recipients' conduct.

301. The violation of section 631(a) constitutes an invasion of privacy sufficient to confer Article III standing. Unless enjoined, Defendant will continue to commit the illegal acts alleged here. Plaintiffs continue to be at risk because she frequently uses the internet to search for information about products or services. She continues to desire to use the internet for that purpose, including for the purpose of acquiring healthcare services online. Plaintiffs also continue to desire to use Defendant's Website in the future but has no practical way to know if her website communications will be monitored or recorded by the Pixel Information Recipients.

302. Plaintiffs and Class Members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and other Class Members, prays for judgment in their favor and against Defendant as follows:

A. an Order certifying the Nationwide Class, Florida Subclass, and California Subclass, and appointing Plaintiffs and their Counsel to represent the Classes;

B. equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

D. an award of all damages available at equity or law, including, but not limited to, actual, consequential, punitive, statutory and nominal damages, as allowed by law in an amount to be determined;

E. an award of attorney fees, costs, and litigation expenses, as allowed by law;

F. prejudgment interest on all amounts awarded and

G. all such other and further relief as this Court may deem just and proper.

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@almeidalawgroup.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
tbean@sirillp.com

**pro hac vice admission anticipated*

Attorneys for Plaintiffs & the Classes