ALMEIDA LAW GROUP LLC
David S. Almeida*
John R. Parker, Jr. (CA No. 257761)
3550 Watt Avenue, Suite 140
Sacramento, California 95821
(916) 616-2936
david@almeidalawgroup.com
jrparker@almeidalawgroup.com

MIGLIACCIO & RATHOD LLP
Nicholas Migliaccio*
412 H St. NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730
nmigliaccio@classlawdc.com

Attorneys for Plaintiffs & the Classes

**Additional Attorneys on Signature Page*

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA

B.C., M.D., A.F., K.S.B. & A.W., *individually and on behalf of all others similarly situated*, Plaintiffs, v. WISP, INC., Defendant.	**Case No.** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs B.C., M.D., A.F., K.S.B. and A.W., individually and on behalf of all others similarly situated ("Plaintiffs"), by and through undersigned counsel, hereby allege the following against Defendant WISP, INC., a Delaware corporation ("Wisp" or "Defendant"). Facts pertaining to Plaintiffs and their experiences and circumstances are alleged based upon personal knowledge and all other facts herein are alleged based upon the investigation of counsel and upon information and good faith belief.[1]

NATURE OF THE ACTION

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

2. Simply put, if people do not (or cannot) trust that their sensitive information will be kept private and secure, they may be less likely to seek medical treatment which can lead to much more serious health consequences down the road. In addition, protecting medical information and making sure it is kept confidential and not

---

[1] Given the sensitive medical information at issue in this case, Plaintiffs file their Complaint with initials to protect their privacy and themselves from harassment, injury, ridicule or personal embarrassment. *See, e.g.*, *Does I thru XXIII v. Advanced Textile Corp.*, 214 F.3d 1058, 1067–68 (9th Cir. 2000) (discussing the standard in the Ninth Circuit for plaintiffs to proceed with pseudonyms) (internal citation & quotation omitted); *Smith v. United Healthcare Ins. Co.*, 2019 WL 3238918, at *7 (N.D. Cal. July 18, 2019) (allowing plaintiff to proceed under pseudonym).

[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*, WIRED (Nov. 16, 2022), available at https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited Nov. 21, 2023); Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited Nov. 21, 2023).

disclosed to any unauthorized entities is vitally necessary to maintain public trust in the healthcare system as a whole.

3. The need for data privacy, security and transparency is particularly acute when it comes to the rapidly expanding world of digital telehealth providers. Of all the information the average internet user shares with technology companies, health data—and especially sexual and reproductive health data–is some of the most valuable and controversial.[3]

4. WISP is a telehealth company that provides primary care, sexual health services and prescription refills as well as markets and sells birth control medications and treatments for sexually transmitted diseases, herpes, urinary tract and yeast infections as well as many other sensitive sexual and reproductive health issues.

5. In order to market and sell these services, Wisp owns, controls and maintains a website https://hellowisp.com/ (the "Website"), which requires individuals to share highly sensitive individually identifiable health information ("IIHII") and protected health information ("PHI" and with IIHI, "Private Information") in order to, among other things, create accounts and participate in personal health screenings and receive treatment plans.[4]

[3] Protected and highly sensitive medical information collected by telehealth companies includes many categories from intimate details of an individual's conditions, symptoms, diagnoses and treatments to personally identifying information to unique codes which can identify and connect individuals to the collecting entity. *See* Molly Osberg & Dhruv Mehrotral, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), available at https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137 (last visited Nov. 21, 2023).

[4] WISP purports to take privacy and security seriously and represents that it complies with all relevant privacy and HIPAA regulations in the U.S. *See* WISP Privacy Policy (updated as of May 24, 2023), available at https://hellowisp.com/privacy (last visited Nov. 21, 2023).

6. In order to acquire the highly valuable Private Information of its users, customers and patients (the "Users"), WISP installed and configured "pixels" and similar tracking technologies on its Website.

7. Invisible to the naked eye, pixels—which are configured by the website owner, here, WISP—collect and transmit information from Users' browsers to unauthorized third parties including, but not limited to, Meta Platforms, Inc. d/b/a Facebook, Google, Bing/Microsoft and TikTok Inc. (collectively, the "Pixel Information Recipients").[5]

8. Through the use of these pixels, cookies and other invisible tracking technologies,[6] WISP's Website directs Users' private communications to automatically

[5] *See* Colin Lecher & Ross Teixeira, *Facebook Watches Teens Online As They Prep For College*, THE MARKUP (Nov. 22, 2023), available at https://themarkup.org/pixel-hunt/2023/11/22/facebook-watches-teens-online-as-they-prep-for-college#:~:text=After%20signing%20into%20their%20ACT,re%20registering%20for%20the%20ACT (stating that "[b]usinesses embed the pixel on their own websites voluntarily, to gather enough information on their customers so they can advertise to them later on Meta's social platforms") (last visited Nov. 27, 2023).

[6] Upon information and good faith belief, WISP also installed and implemented the Facebook Conversions Application Programming Interface ("Conversions API") on its servers. Conversions API serves the same purpose as pixels in that it collects and transmits Private Information to, for example, Facebook. Unlike the Pixels, however, Conversions API functions from WISP's servers and therefore cannot be stymied by use of anti-Pixel software or other workarounds.

Further, while this Complaint primarily focuses on how the Facebook Pixel collected and disclosed Users' Private Information on the Website, other secret tracking technologies embedded by WISP, such as Google Analytics, Google tag manager and the TikTok and Bing tracking codes, also collect such Private Information, and the respective tech companies have the capability to link it to specific user profiles they have built. For example, Google stores Users' logged-in identifier on non-Google website in its logs. Whenever a User logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the User's browsing activities on that website. Google

be sent to the servers of the corresponding Pixel Information Recipients. This collection and disclosure occurs on every webpage in which WISP installed pixels and/or for which it enabled Conversions API.

9. Once Users' Private Information is collected and transmitted to, *e.g.*, Facebook, it is combined with a User's Facebook profile and all of the information about this person is accessible via the User's unique Facebook ID ("FID").[7] Then, completely unencumbered by any pretense of restriction or regulation, the Pixel Information Recipients, in turn, use that Private Information for various business purposes, including using such information to "improve" advertisers' ability to target specific demographics and selling such information to third-party marketers who target those Users online (*i.e.*, through their Facebook, Instagram, TikTok, Gmail, Microsoft account, and other social media and personal accounts).[8]

10. The Private Information that pixels, Conversions API and other third-party tracing codes gathered from WISP's Website and sent to the Pixel Information Recipients included the Private Information that Users submitted to WISP's Website, including for example, particular health conditions, types of health treatment sought and/or received, name, age and other confidential IIHI and PHI. That is, although

---

further logs all such data (private and non-private) within the same logs and uses these data for serving personalized ads.

[7] Facebook tracks and collects data even on people who do not have a Facebook account or have deactivated their Facebook accounts. And those individuals can find themselves in an even worse situation because even though their Private Information is sent to Facebook (without consent) since they do not 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."

[8] *See* Lecher & Teixeira, *supra*, note 2 ("Along with encouraging businesses to spend ad dollars, Facebook also receives the transmitted data, and can use it to hone its algorithms. Facebook can also use data from the pixel to link website visitors to their Facebook accounts, meaning businesses can reach the exact people who visited their sites. The pixel collects data regardless of whether the visitor has an account.").

WISP's patients understandably had a reasonable expectation of privacy as they used the Website, those Users were unknowingly providing their Private Information to WISP as they (i) navigated the Website, (ii) created patient accounts, (iii) completed health assessments and questionnaires, (iv) researched doctors and other health-related services providers, (v) reviewed conditions and available treatments, (vi) researched prescriptions, (vii) purchased treatment options and (viii) made and managed appointments.

11. WISP begins tracking its customers from the moment they land on the main Website, https://hellowisp.com/, via Meta Pixels with ID numbers 1863436503950868 and 253897343916108. The Pixels are configured to capture a number of "events" as the user browses the website, registers as a customer, and/or purchases products including, but not limited to, "PageView," "SubscribedButtonClick," "ViewContent," and "AddToCart."

12. These events disclose the user/customer's specific medical condition, the fact that the user is searching for specific treatments for their sensitive medical condition, WISP's specific treatment recommendations for the customer upon their completion of a symptoms quiz (such as, for example, an "STD consult"), and the fact that the user is purchasing WISP products to treat their specific medical condition—along with the customer's email, zip code, their unique Facebook ID and other personal identifiers such as their internet protocol ("IP") address, and even specific purchase details such as whether the customer wants to pick up their purchase at a local pharmacy or have it delivered to their home.[9]

13. Plaintiffs and Class Members who visited and used WISP's Website understandably thought they were communicating *only* with their trusted healthcare providers. But by employing third-party trackers, which obtain detailed information about its customers' medical information and sexual health, WISP effectively bartered

[9] As discussed, *infra*, each of these categories of information constitutes PHI.

the private medical information of its patients for more detailed analytics of its Users to increase its revenues and profits.

14. To make matters worse, WISP has ***not*** informed those Users of the unauthorized disclosure of their Private Information as many other healthcare and telehealth entitles who have utilized similar tracking technology to collect and disclose Private Information to third parties have done.[10]

15. Despite numerous warnings from federal regulators (not to mention several FTC enforcement actions against telehealth companies for similar conduct), WISP designed and maintained its Website so that Users would be required to submit Private Information in order to participate in health assessments and other health-related services, review treatments offered by Defendant for their medical conditions, purchase treatment options and create accounts, among many other things.

16. The reason that WISP went to these lengths to obtain this sensitive Private Information is, quite simply, because its patients would ***not*** provide it if they were informed and given a choice. That is, if WISP told its patients that by using its Website their sensitive Private Information would be collected and disseminated to Facebook and/or other third-party platforms, they would not consent to that—or they would demand significant compensation for the use of their private and valuable health information in this manner.

---

[10] In contrast to WISP, in the last year, several medical providers that installed the Meta Pixel on their Web Properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf; Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies,* FIERCE HEALTHCARE (October 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3; *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWSWIRE (August 19, 2022), https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html.

17. As detailed herein, WISP owed common law, contractual, statutory and regulatory duties to keep its Users' Private Information safe, secure and confidential. Furthermore, by obtaining, collecting, using and deriving a benefit from their Private Information, WISP assumed legal and equitable duties to patients to protect and safeguard their Private Information from unauthorized disclosure. WISP, however, failed in its obligations and promises by utilizing pixel, Conversions API, and/or other tracking codes to collect and divulge Plaintiffs' and Class Members' Private Information with the Pixel Information Recipients.[11]

18. As a result, Plaintiffs and Class Members have suffered numerous compensable injuries including (i) invasion of privacy, (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the transmissions of their Private Information to the Pixel Information Recipients, (iii) loss of the benefit of the bargain, (iv) diminution of value of the disclosed Private Information, (v) statutory damages and (vi) the continued and ongoing risk to their Private Information.

19. Plaintiffs seek to remedy these harms and therefore bring this class action lawsuit on behalf of all similarly situated individuals whose Private Information was disclosed to the Pixel Information Recipients through WISP's unauthorized use of pixels, Conversions API and/or other similar tracking technologies. Plaintiffs assert individual and representative claims for: (i) negligence; (ii) invasion of privacy—

[11] WISP breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure the Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share patients' Private Information; (iii) failing to obtain the consent of patients, including Plaintiffs and Class Members, to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through the Pixels and Conversions API; (v) failing to warn Plaintiffs and Class Members of such sharing and disclosures; (vi) otherwise failing to design and monitor the Website to maintain the confidentiality and integrity of patients' Private Information.

intrusion upon seclusion, (iii) breach of confidence; (iv) unjust enrichment; (v) breach of implied contract; (vi) violations of the Electronics Communication Privacy Act ("ECPA"), 18 U.S.C. § 2511(1); (vii) Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*; (viii) violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et. seq.*; (ix) violation of the California Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code § 1750, *et seq.*; (x) violation of the California Unfair Competition Law ("UCL"), Unlawful and Fraudulent Business Practices, Cal. Bus. & Prof. Code § 17200, *et seq.*; (xi) violation of the California Unfair Competition Law ("UCL"), Unfair Business Practices, Cal. Bus. & Prof. Code § 17200, *et seq.*; (xii) violation of the North Carolina's Unfair & Deceptive Practices Act, N.C. Gen. Stat. § 75-1.1, *et seq.*; (xiii) violation of the Arkansas Deceptive Trade Practices Act, Ark. Code Ann § 4-88-101, *et seq.*; (xiv) violation of the District of Columbia Consumer Protection Procedures Act, D.C. Code § 28-3901, *et seq.*; (xv) violation of the Tennessee Trade Practices Act, Tennessee Code Annotated § 47-25-101, *et seq.*; (xvi) violation of the Virginia Consumer Protection Procedures Act, Virginia Code Ann. § 59.1-196, *et seq.*

PARTIES

A. Plaintiffs.

20. Plaintiff B.C. is a citizen of the State of Tennessee residing in Ripley and brings this action in an individual capacity and on behalf of all others similarly situated.

21. Plaintiff M.D. is a citizen of the District of Columbia and brings this action in an individual capacity and on behalf of all others similarly situated.

22. Plaintiff A.F. is a citizen of the State of Virigina residing in Norfolk and brings this action in an individual capacity and on behalf of all others similarly situated.

23. Plaintiff K.S.B. is a citizen of the State of Arkansas residing in Cabot and brings this action in an individual capacity and on behalf of all others similarly situated.

24. Plaintiff A.W. is a citizen of the State of North Carolina residing in Durham and brings this action in an individual capacity and on behalf of all others similarly situated.

B. Defendant Wisp, Inc.

25. Defendant Wisp, Inc. is a foreign corporation incorporated in Delaware and headquartered at 28 Baker St B, San Francisco, California, 94117.

JURISDICTION & VENUE

26. 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.

27. 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 are citizens of different states than Defendant.

28. This Court has personal jurisdiction over WISP because it operates and maintains their principal place of business in this judicial district. Further, WISP is authorized to and regularly conduct business in this judicial district and make decisions regarding corporate governance and management of the Website in this judicial district, including decisions regarding the privacy of Users' Private Information and the incorporation of the Pixels, Conversions API and other tracking technologies.

29. Venue is proper in this judicial 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 judicial district, including decisions made by WISP's governance and management personnel or inaction by those individuals that led to the unauthorized sharing of Users' Private Information; WISP's principal place of business is located in this judicial

district; WISP collects and divulges Users' Private Information in this judicial district and WISP caused harm to Class Members residing in this District.

COMMON FACTUAL ALLEGATIONS

A. Federal Regulators Make Clear that the Use of Tracking Technologies to Collect and Divulge Private Information Without Informed Consent is Illegal.

30. This surreptitious collection and divulgence of Private Information is an extremely serious data security and privacy issue. Both the Federal Trade Commission and the Office for Civil Rights of the Department of Health and Human Services ("HHS") have, in recent months, reiterated the importance of and necessity for data security and privacy concerning health information.

31. For instance, the 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."***[12]

32. 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:

---

[12] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases,* THE FTC BUSINESS BLOG (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 Nov. 20, 2023).

> ***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***.[13]

33. The federal government is taking these violations of health data privacy and security seriously as the recent high-profile FTC settlements against several telehealth companies.

34. For example, earlier this year the FTC imposed a $1.5 million penalty on GoodRx for violating the FTC Act by sharing its customers' sensitive personal health information with advertising companies and platforms including Facebook, Google and Criteo, and proposed a $7.8 million settlement with the online counseling service BetterHelp, resolving allegations that the company shared customer health data with Facebook and Snapchat for advertising purposes. And Easy Healthcare was ordered to

[13] *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).

pay a $100,000 civil penalty for violating the Health Breach Notification Rule when its ovulation tracking app Premon shared health data for advertising purposes.[14]

35. Even more recently, in July 2023, federal regulators sent a letter to approximately 130 healthcare providers warning them about the use of online tracking technologies that could result in unauthorized disclosures of Private Information to third parties. The letter highlighted the "risks and concerns about the use of technologies, such as the Meta/Facebook Pixel and Google Analytics, that can track a user's online activities," and warned about "[i]mpermissible disclosures of an individual's personal health information to third parties" that could "result in a wide range of harms to an individual or others." According to the letter, "[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more."[15]

36. Moreover, the Office for Civil Rights ("OCR") at HHS has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered*

---

[14] *See* How FTC Enforcement Actions Will Impact Telehealth Data Privacy, https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy (last visited Nov. 22, 2023); *See* Allison Grande, *FTC Targets GoodRx In 1st Action Under Health Breach Rule*, Law360 (Feb. 1, 2023), available at www.law360.com/articles/1571369/ftc-targets-goodrx-in1st-action-under-health-breach-rule?copied=1 ("The Federal Trade Commission signaled it won't hesitate to wield its full range of enforcement powers when it dinged GoodRx for allegedly sharing sensitive health data with advertisers, teeing up a big year for the agency and boosting efforts to regulate data privacy on a larger scale."); https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising; https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc (last visited Nov. 27, 2023).

[15] *See* https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf (last visited Nov. 26, 2023).

Entities and Business Associates (the "OCR Bulletin"), that the unlawful transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[16]

37. The OCR Bulletin reminds healthcare organizations regulated under the HIPAA that they may use third-party tracking tools, such as Google Analytics or Pixels *only in a limited way*, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.[17]

38. The OCR Bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.*** Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual***

[16] OCR Bulletin, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html, HHS.GOV (emphasis added) (last visited Nov. 25, 2023).

[17] *See id*.

> ***seeks medical treatment.*** While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***[18]

39. Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to monetize their Users' Private Information. For instance, THE MARKUP reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment.[19]

40. And, in the aptly titled report *"Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, a joint investigation by STAT and The Markup of 50 direct-to-consumer telehealth companies, reported that telehealth companies or virtual care websites were providing sensitive medical information they collect to the world's largest advertising platforms.[20]

---

[18] *Id.* (emphasis added).

[19] *See* Feathers, Fondrie-Teitler, Waller & Mattu, THE MARKUP, *supra,* note 2.

[20] Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, *"Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies: An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech's tracking tools*, THE MARKUP (Dec. 13, 2022), available at https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies (last visited Nov. 21, 2023).

41. Many telehealth sites, including WISP, had at least one tracker—from Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn and/or Pinterest—that collected patients' answers to medical intake questions.[21]

B. The Tracking Pixels.

42. A "pixel" is a piece of code that "tracks the people and the types of actions they take"[22] 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 more.

43. 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.

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

42. The Pixels can also share the user's identifying information for easy tracking via the "cookies"[23] stored on their computer by any of the Pixel Information

---

[21] *See id.* (noting that "[t]rackers on 25 sites, including those run by industry leaders Hims & Hers, Ro, and Thirty Madison, told at least one big tech platform that the user had added an item like a prescription medication to their cart, or checked out with a subscription for a treatment plan").

[22] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Nov. 15, 2023).

[23] "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 Nov. 25, 2023).

Recipients with which they have an account. For example, Facebook stores or updates a Facebook-specific cookie every time a person accesses their Facebook account from the same web browser.

43. 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.

44. 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.

45. Businesses embed the pixel on their own websites voluntarily, to gather enough information on their customers so they can advertise to them later on Meta's social platforms, Facebook and Instagram.[24]

46. Defendant has utilized Pixels and other tracking technologies since at least January 2017.

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

C. Conversions API.

48. The Facebook Conversions API and similar tracking technologies allow businesses to send web events, such as clicks, form submissions, keystroke events, and other user actions performed by the user on the Website, from their own servers to Facebook and other third parties.[25]

49. Conversions API creates a direct and reliable connection between

[24] *See* Lecher & Teixeira, *Facebook Watches Teens Online As They Prep For College*, THE MARKUP, *supra*, note 5.

[25] https://revealbot.com/blog/facebook-conversions-api/ (last visited Nov. 25, 2023).

marketing data (such as a user's private and confidential actions on Defendant's Website) from Defendant's server to Facebook.[26] In doing so, Defendant stores Plaintiffs' and Class Members' Private Information on their own server and then transmits it to unauthorized third parties.

50. Conversions API is an alternative method of tracking versus the Facebook Pixel because no privacy protections on the user's end can defeat it. This is because it is "server-side" implementation of tracking technology, whereas the Pixels are "client-side," *i.e.*, executed on users' computers in their web browsers.

51. Because Conversions API is server-side, it cannot access the Facebook-specific cookie to retrieve the user's Facebook ID.[27] Therefore, other roundabout methods of linking the user to their Facebook account are employed by Facebook.[28] For example, Facebook has an entire page within its developers' website about how to de-duplicate data received when both the Facebook Pixel and Conversions API are executed.[29]

---

[26] https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Nov. 25, 2023).

[27] "Our systems are designed to not accept customer information that is unhashed Contact Information, unless noted below. Contact Information is information that personally identifies individuals, such as names, email addresses, and phone numbers, that we use for matching purposes only." *See* https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/ (last visited Nov. 25, 2023).

[28] "Sending additional customer information parameters may help increase Event Match Quality. Only matched events can be used for ads attribution and ad delivery optimization, and the higher the matching quality, the better." https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req- rec-params (last visited Nov. 25, 2023).

[29] *See* https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel- and-server-events (last visited Nov. 25, 2023).

52. Conversions API tracks the user's website interaction, including Private Information being shared, and then transmits this data to Facebook and other third parties. Facebook markets Conversions API as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."

53. Defendant installed the Pixels and Conversion API, as well as other tracking technologies, on many (if not all) of the webpages within the Website and programmed or permitted those webpages to surreptitiously share patients' private and protected communications with the Pixel Information Recipients—communications that included Plaintiffs' and Class Members' Private Information.

D. Defendant's Method of Transmitting Users' Private Information via Pixel & Conversions API.

54. 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 a computer, tablet, or smartphone) accesses web content through a web browser (*e.g.*, Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

55. Every website is hosted by a computer "server" that holds the website's contents. The entity(ies) in charge of the website exchange communications with users' client devices as their web browsers query the server through the internet.

56. Web communications consist of Hypertext Transfer Protocol ("HTTP") or Hypertext Transfer Protocol Secure ("HTTPS") requests and HTTP or HTTPS responses, and any given browsing session may consist of thousands of individual HTTP requests and HTTP responses, along with corresponding cookies:

a. **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. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF for filing a motion to a court.)

b. **Cookies**: a small text file that can be used to store information on the client device that 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.

c. **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.

57. A patient's HTTP request essentially asks the Defendant's Website to retrieve certain information (such as a set of health screening questions). The HTTP response sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the participant's screen as they navigate Wisp's Website.

58. Every website is comprised of Markup and "Source Code." Source Code is a simple set of instructions that commands the website user's browser to take certain actions when the webpage first loads or when a specified event triggers the code.

59. 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 web browser's user.

60. The Pixels are Source Code that does just that—they surreptitiously transmit a Website user's communications and inputs to the corresponding Pixel Information Recipient much like a traditional wiretap. When individuals visit Defendant's Website via an HTTP request to Defendant's server, Defendant's server

sends an HTTP response (including the Markup) that displays the webpage visible to the user, along with Source Code (including the Pixels).

61. Thus, Defendant is, in essence, handing its patients a tapped phone and, once the webpage is loaded into the patient's browser, the software-based wiretaps are quietly waiting for private communications on the webpage to trigger the Pixels, which then intercept those communications intended only for Defendant and transmits those communications to the corresponding Pixel Information Recipient.

62. Third parties like the Pixel Information Recipients 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 user associated with the information intercepted (in this case, highly sensitive Private Information).

63. Defendant intentionally configured Pixels installed on its Website to capture both the "characteristics" of individual patients' communications with the Defendant's Websites (*i.e.*, 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).

64. Defendant also deposits cookies named _fbp, _ga_, and _gid 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. And 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.

65. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Defendant's use of the Facebook Pixel. 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 and _gid cookies operate similarly as to Google.

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

E. Facebook's Platform & its Business Tools.

67. 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.[30]

68. 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.

69. Facebook's Business Tools, including the Facebook Pixel, 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.

70. 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") and metadata, button clicks, etc.[31]

---

[30] 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 (last visited Nov. 25, 2023).

[31] *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Nov. 25, 2023); *see*, META PIXEL, GUIDES, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/ (last visited Nov. 15, 2023); *see also* BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142 (last visited Nov. 25, 2023); META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Nov. 25, 2023).

71. Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[32]

72. One such Business Tool is the Facebook Pixel, which "tracks the people and type of actions they take" on a webpage in which the Pixel has been installed.[33]

73. When a user accesses a webpage that is hosting the Facebook Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent from the user's browser to Facebook's server.

74. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is 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.

75. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients' 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 unique personal identifiers including email address and/or phone number.

76. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[34] Plaintiffs' and

---

[32] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142, FACEBOOK. COM (last visited Nov. 25, 2023); *see also* META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[33] RETARGETING, https://www.facebook.com/business/goals/retargeting, FACEBOOK. COM (last visited Nov. 25, 2023).

[34] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-

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.

77. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. When 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.

78. The pixel collects data regardless of whether the visitor has an account. Facebook maintains "shadow profiles" on users without Facebook accounts and links the information collected via the Facebook Pixel to the user's real-world identity using their shadow profile.[35]

79. When Facebook receives the transmitted data, it can use it to hone its algorithms.[36]

80. A user's Facebook ID 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 Profile 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

---

identification/index.html (last visited Nov. 27, 2023).

[35] *See* Russell Brandom, *Shadow Profiles Are The Biggest Flaw In Facebook's Privacy Defense*, TheVerge.com (Apr 11, 2018), *available at* https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (last visited Nov. 25, 2023).

[36] *See Facebook Watches Teens Online As They Prep For College*, *supra,* note 5.

www.facebook.com/ followed by the c_user ID.

81. The Private Information disclosed via the Pixel allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought. Facebook then uses that information to sell advertising to Defendant and other advertisers and/or sells that information to marketers who will online target Plaintiffs and Class Members.

82. With substantial work and technical know-how, internet users can sometimes circumvent the browser-based wiretap technology of the Pixels. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that even savvy users cannot evade. Facebook's workaround is called Conversions API.

83. Conversions API is effective because it transmits directly from the host server and does not rely on the user's web browser.

84. Thus, the communications between patients and Defendant, which are necessary to achieve the purpose of Defendant's Website, are received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.[37]

85. The Pixel Information Recipients track user data and communications for their own marketing purposes and for the marketing purposes of the website owner.

---

[37] Although prior to discovery there is no way to confirm that Defendant has implemented Conversions API or another workaround (as that would require accessing the host server), Facebook instructs website owners like Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose." *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Nov. 25, 2023). Thus, it is reasonable to infer that Wisp is utilizing the Conversions API workaround.

Ultimately, the purpose of collecting user data is to make money.

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

87. In this case, Defendant employed the Pixels and Conversions API, among other tracking technologies, to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to Facebook and the other Pixel Information Recipients.

88. In sum, the Pixels and other tracking technologies on the Website transmitted Plaintiffs' and Class Members' highly sensitive communications and Private Information to the corresponding Pixel Information Recipient, which communications contained private and confidential medical information.

89. These transmissions were performed without Plaintiffs' or Class Members' knowledge, consent, or express written authorization.

F. Wisp's Use of the Pixels Violated Their Own Privacy Policies.

90. Defendant breached Plaintiffs' and Class members' right to privacy by unlawfully disclosing their Private Information to the Pixel Information Recipients.

91. Specifically, Plaintiffs and Class members 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.

92. Specifically, Defendant did not inform Plaintiffs that it shared their Private Information with Facebook and the other Pixel Information Recipients. Moreover, Defendant's Privacy Policy did not state that user and patient Private Information will be shared with Facebook or other unauthorized third parties. To the contrary, Defendant acknowledges that health information it receives from its customers may be "protected health information" under HIPAA, the Health Information Technology for Economic and Clinical Health Act, and state privacy laws and regulations, and claims to comply

with these federal and state laws and regulations "to ensure that your protected health information is appropriately safeguarded."[38]

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

G. Wisp's Use of the Pixels Violates HIPAA.

94. 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.[39]

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

96. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

97. The Privacy Rule broadly defines "protected health information" as individually identifiable health information 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.

---

[38] WISP Privacy Policy, https://hellowisp.com/privacy (last visited Nov. 22, 2023).

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

98. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

A. Names;

…

J. Account numbers;

…

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers; … and

P. Any other unique identifying number, characteristic, or code… and" the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 164.514.

99. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of PHI without authorization. 45 C.F.R. §§ 160.103, 164.502.

100. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be PHI.

101. HHS has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a

phonebook because it is not related to health data, "[i]f such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI."[40]

102. Consistent with this restriction, the HHS has issued marketing guidance that provides, "[w]ith limited exceptions, the [Privacy] Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list."[41]

103. Here, as described *supra*, Defendant provided patient information to third parties in violation of the Privacy Rule – and its own Privacy Policy.

104. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(c), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1) – which Defendant failed to do.

105. WISP further failed to comply with other HIPAA safeguard regulations as follows:

a. Failing to ensure the confidentiality and integrity of

---

[40] *See 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 Nov. 25, 2023).

[41] *Marketing*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html (last visited Nov. 15, 2023).

electronic PHI that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. section 164.306(a)(1);

b. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);

c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendant in violation ofc45 C.F.R. section 164.308(a)(6)(ii);

d. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. section 164.306(a)(2);

e. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3) and

f. Failing to design, implement, and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

106. Commenting on a June 2022 report discussing the use of Pixels by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it … It is quite likely a HIPAA violation."[42]

[42] '*Deeply Troubled*': *Security experts worry about Facebook trackers on hospital sites*, ADVISORY BOARD, https://www.advisory.com/daily-briefing/2022/06/17/data-trackers (last visited Nov. 25, 2023).

107. Defendant's use of third-party tracking code on its Website is a violation of Plaintiffs' and Class Members' privacy rights under federal law. While Plaintiffs do not bring a claim under HIPAA itself, this violation demonstrates Defendant's wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

H. Defendant's Use of the Pixels Violates OCR Guidance.

108. In addition, the government has issued guidance warning that tracking technologies like the Pixels may come up against federal privacy law when installed on healthcare websites.

109. As mentioned previously, healthcare organizations regulated under the HIPAA may use third-party tracking tools, such as Google Analytics or Pixels *only in a limited way*, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.[43]

110. According to the Bulletin, Defendant has violated HIPAA rules by implementing the Pixels.[44]

111. Plaintiffs and Class Members face the same risks warned of by the HHS OCR in the OCR Bulletin.

112. Defendant has shared Plaintiffs' and Class Members' Private Information including health conditions for which they seek treatments; treatments and/or medications sought; the frequency with which they take steps to obtain healthcare for certain conditions; and their unique personal identifiers. This information is, as described in the OCR Bulletin, "highly sensitive."

113. The OCR Bulletin goes on to make clear how broad the government's view of protected information is as it explains:

---

[43] *See* OCR Bulletin, *supra*, note 16.

[44] *See id*. ("disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures").

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code.***[45]

114. Defendant's sharing of Private Information to the Pixel Information Recipients violated Plaintiffs' and Class Members' rights.

I. Wisp Violated Industry Standards.

115. It is a cardinal rule that a medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship.

116. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

117. AMA Code of Ethics Opinion 3.1.1 provides:

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

118. AMA Code of Medical Ethics Opinion 3.2.4 provides:

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

[45] *Id.* (emphasis added).

119. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must: (c) Release patient information only in keeping ethics guidelines for confidentiality.[46]

120. Defendant's use of the Pixels also violates data security guidelines. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

121. The FTC's October 2016 publication *Protecting Personal Information: A Guide for Business*[47] established cyber-security guidelines for businesses. These guidelines state that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network vulnerabilities; and implement policies to correct any security problems.

122. As discussed herein, the FTC has since also made clear that healthcare companies should not use tracking technologies to collect sensitive health information and disclose it for marketing and advertising purposes without consumers' informed consent.[48]

123. In fact, as also described above, the FTC has recently brought enforcement

---

[46] AMA Principles of Medical Ethics: I, IV, *Chapter 3: Opinions on Privacy, Confidentiality & Medical Records*, https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf, American Medical Association (last visited Nov. 25, 2023).

[47] Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 25, 2023).

[48] *See* Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases, supra,* note 12.

actions against several healthcare companies, including Premom, BetterHelp, GoodRx and Flow Health for conveying information—or enabling an inference—about their consumers' health to unauthorized third parties without the consumers' consent.

124. Just like the telehealth companies fined by the FTC in recent years, Defendant failed to implement these basic, industry-wide data security practices.

J. Users' Reasonable Expectation of Privacy.

125. Plaintiffs and Class members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

126. Indeed, at all times when Plaintiffs and Class Members provided their IIHI 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.

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

128. 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.[49]

129. Personal data privacy and obtaining consent to share Private Information are material to Plaintiffs and Class members.

K. Unique Personal Identifiers are Protected Health Information.

130. While not all health data is covered under HIPAA, the law specifically

[49] *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 Oct. 9, 2023).

applies to healthcare providers, health insurance providers and healthcare data clearinghouses.[50]

131. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted, and there are approximately 18 HIPAA Identifiers that are considered PII. This information can be used to identify, contact or locate a single person or can be used with other sources to identify a single individual. These HIPAA Identifiers, as relevant here, include names, addresses, dates related to an individual, telephone numbers, email addresses, medical record numbers, health plan beneficiary numbers, web URLs, and IP addresses.[51]

132. WISP improperly disclosed Plaintiffs' and Class Members' computer IP addresses to the Pixel Information Recipients through their use of the Pixels *in addition to* unique personal identifiers such as phone numbers, email addresses, dates of birth, Defendant's client ID numbers, services selected, assessment responses, patient statuses, medical conditions, treatments, provider information, and appointment information. And every data packet sent by a tech company's tracker includes the user's IP address, which is one of several unique identifiers that explicitly qualifies for health data for protection under HIPAA.[52]

133. An IP address is a number that identifies the address of a device connected

---

[50] *See* Alfred Ng & Simon Fondrie-Teitler, *This Children's Hospital Network Was Giving Kids' Information to Facebook* (June 21, 2022), available at https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook (last visited March 17, 2023) (stating that "[w]hen you are going to a covered entity's website, and you're entering information related to scheduling an appointment, including your actual name, and potentially other identifying characteristics related to your medical condition, there's a strong possibility that HIPAA is going to apply in those situations").

[51] https://www.luc.edu/its/aboutus/itspoliciesguidelines/hipaainformation/the18hipaaidentifiers/ (last visited Nov. 27, 2023).

[52] *See* Feathers, Palmer (STAT) & Fondrie-Teitler, MARKUP, *supra*, note 20.

to the Internet. IP addresses are used to identify and route communications on the Internet. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

134. Facebook tracks every IP address ever associated with a Facebook user (and with non-users through shadow profiles). Google also tracks IP addresses associated with Internet users.

135. Facebook, Google, and other third-party marketing companies track IP addresses for targeting individual homes and their occupants with advertising.

136. Under HIPAA, an IP address is considered personally identifiable information, defining personally identifiable information as including "any unique identifying number, characteristic or code" and specifically listing IP addresses among examples. 45 C.F.R. § 164.514 (2).

137. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *see also*, 45 C.F.R. § 164.514(b)(2)(i)(O).

138. Consequently, Defendant's disclosure of Plaintiffs' and Class Members' IP addresses violated HIPAA and industry-wide privacy standards.

L. WISP Was Enriched & Benefitted from the Use of Tracking Technologies that Enabled the Unauthorized Disclosures Alleged Herein.

139. The purpose of the use of the Pixels and other tracking technologies on Defendant's Website was to improve marketing and thereby boost revenues.

140. In exchange for disclosing the Private Information of their accountholders and patients, Defendant is compensated by the Pixel Information Recipients in the form of enhanced advertising services and more cost-efficient marketing on their platform.

141. Defendant was advertising their services through Facebook, for one, and the Pixels were used to "help [Defendant] understand which types of ads and platforms

are getting the most engagement[.]"[53]

142. Retargeting is a form of online marketing that targets users with ads based on previous internet communications and interactions.

143. Defendant retargeted patients and potential patients to get more people to use their services. These patients include Plaintiffs and Class Members.

144. Thus, utilizing the Pixels benefits Defendant by, among other things, reducing the cost of advertising and retargeting.

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

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

147. 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.[54]

148. Similarly, CNBC published an article in 2019 in which it observed that "[p]atient 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."[55]

---

[53] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Nov. 25, 2023).

[54] *See* https://time.com/4588104/medical-data-industry/ (last visited Nov. 25, 2023).

[55] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Nov. 25, 2023).

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

150. Defendant gave away Plaintiffs' and Class Members' Private Information without permission.

151. The unauthorized access to Plaintiffs' and Class Members' private and Personal Information has diminished the value of that information, resulting in harm to Website users, including Plaintiffs and Class Members.

152. Plaintiffs suffered damages in the form of (a) invasion of privacy; (b) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the invasion of privacy; (c) diminution of value of the Private Information; (d) statutory damages; (e) the continued and ongoing risk to their Private Information; (f) lost benefit of the bargain; and (g) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiffs' medical conditions and other confidential information they communicated to Defendant via the Website.

153. Plaintiffs have a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

REPRESENTATIVE PLAINTIFFS' ALLEGATIONS

A. PLAINTIFF B.C.

154. In or around July 2022, Plaintiff B.C. utilized Defendant's Website on her personal electronic devices to create an account, research conditions and treatments, search for doctors and schedule appointments.

155. While seeking those services and treatments, Wisp required Plaintiff B.C. to provide—and Plaintiff B.C. provided—personal health information including her

name, email address and medical conditions.

156. Additionally, Wisp required Plaintiff B.C. to provide additional PHI including weight, height, blood pressure, whether she was on medications and, if so, which ones, and which of their services she wanted to use.

157. While searching Wisp's specific services, the Website presented numerous guided questions, and then asked Plaintiff B.C. to respond to questions to confirm its diagnosis of her condition.

158. For Plaintiff B.C.'s urinary tract infection ("UTI"), Wisp required Plaintiff B.C. to provide information regarding her medications, and then asked her personal questions regarding burning sensation, bathroom use, how often burning happened, and the history of the infection.

159. Once finished, Wisp would send medication to Plaintiff B.C.'s nearest pharmacy.

160. While Plaintiff B.C. was a user of Wisp's services, she never consented to or authorized the use of her Private Information by third parties or to Defendant enabling third parties to access, interpret, and use such Private Information.

161. Plaintiff B.C. 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.

162. After providing her Private Information to Defendant through the Website, Plaintiff B.C. immediately began seeing health ads targeted to her health conditions disclosed to Defendant as she scrolled through her accounts.

B. PLAINTIFF M.D.

163. Beginning in or around March 2023, Plaintiff M.D. utilized Defendant's Website on her personal electronic devices to request and refill prescriptions. Plaintiff M.D. used Defendant's Website for this purpose approximately 3-4 times, most recently in August 2023.

164. While seeking those services and treatments, Defendant required Plaintiff

M.D. to provide—and Plaintiff M.D. provided—PHI including her name, email address, home address, date of birth, health insurance information, weight, height, allergies, whether she was on medications and, if so, which ones, and which of Defendant's services she wanted to use. Defendant also inquired about whether Plaintiff M.D. had any medical conditions, but Plaintiff M.D. did not have any at that time.

165. For Plaintiff M.D.'s birth control prescription, Defendant required Plaintiff M.D. to provide information regarding which birth control medications Plaintiff M.D. had used in the past and whether she was satisfied with them.

166. Once finished, Defendant would send medication to Plaintiff M.D.'s nearest pharmacy.

167. While Plaintiff M.D. was a user of Defendant's services, she never consented to or authorized the use of her Private Information by third parties or to Defendant enabling third parties to access, interpret, and use such Private Information.

168. Plaintiff M.D. 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.

169. After providing her Private Information to Defendant through the Website, Plaintiff M.D. immediately began seeing health ads targeted to her health conditions disclosed to Defendant as she scrolled through her accounts.

170. For example, these targeted ads included among other ads, Kindbody appointments for fertility, appointments for online therapy and resources for mental health support, antidepressant medications, resources for cancer and skincare clinics.

C. PLAINTIFF A.F.

171. Beginning in or around June 2022, Plaintiff A.F. utilized Defendant's Website on her personal electronic devices to request and refill prescriptions. Plaintiff A.F. used Defendant's Website for this purpose approximately 10 times, most recently in September 2022.

172. While seeking those services and treatments, Defendant required Plaintiff

A.F. to provide—and Plaintiff A.F. provided—PHI including her name, email address, home address, date of birth, health insurance information, medical conditions, weight, height, allergies, whether she was on medications and, if so, which ones, and which of Defendant's services she wanted to use.

173. While searching Defendant's specific services, the Website presented Plaintiff A.F. with numerous questions that she was required to answer to permit Defendant to formulate a diagnosis as to Plaintiff's medical conditions.

174. For Plaintiff A.F.'s vaginal yeast infection and bacterial vaginosis, Defendant required Plaintiff A.F. to provide personal information regarding the ongoing symptoms of these medical issues.

175. Once finished, Defendant would send medication to Plaintiff A.F's nearest pharmacy.

176. While Plaintiff A.F. was a user of Defendant's services, she never consented to or authorized the use of her Private Information by third parties or to Defendant enabling third parties to access, interpret, and use such Private Information.

177. Plaintiff A.F. 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.

178. After providing her Private Information to Defendant through the Website, Plaintiff A.F. immediately began seeing health ads targeted to her health conditions disclosed to Defendant as she scrolled through her accounts.

D. PLAINTIFF K.S.B.

179. Beginning in or around June 2020, Plaintiff K.S.B. utilized Defendant's Website on her personal electronic devices to research conditions and treatments, request or refill prescriptions, and receive telehealth care. Plaintiff K.S.B. used Defendant's Website for these purposes approximately 22 times.

180. While seeking those services and treatments, Defendant required Plaintiff K.S.B. to provide—and Plaintiff K.S.B. provided—PHI including her name, email

address, home address, social security number, date of birth, health insurance information, medical conditions, weight, height, blood pressure, allergies, insurance information, primary care provider and pharmacy, whether she was on medications and, if so, which ones, and which of Defendant's services she wanted to use.

181. While searching Defendant's specific services, the Website presented Plaintiff K.S.B. with numerous questions that she was required to answer to permit Defendant to formulate a diagnosis as to Plaintiff K.S.B.'s medical condition.

182. For Plaintiff K.S.B.'s vaginal yeast infection, Defendant required Plaintiff K.S.B. to provide information regarding her medications, and then asked her personal questions regarding her ongoing symptoms for which she was seeking treatment.

183. Once finished, Defendant would send medication to Plaintiff K.S.B.'s nearest pharmacy.

184. While Plaintiff K.S.B. was a user of Defendant's services, she never consented to or authorized the use of her Private Information by third parties or to Defendant enabling third parties to access, interpret, and use such Private Information.

185. Plaintiff K.S.B. 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.

186. After providing her Private Information to Defendant through the Website, Plaintiff K.S.B. immediately began seeing health ads targeted to her health conditions disclosed to Defendant as she scrolled through her accounts.

E. PLAINTIFF A.W.

187. In or around August 2022, Plaintiff A.W. utilized Defendant's Website on her personal electronic devices to request and refill prescriptions at least on two separate occasions..

188. While seeking those services and treatments, Defendant required Plaintiff A.W. to provide—and Plaintiff A.W. provided—PHI including her name, email address, home address, date of birth, health insurance information, medical conditions,

weight, height, blood pressure, whether she was on medications and, if so, which ones, and which of Defendant's services she wanted to use.

189. For Plaintiff A.W.'s For Plaintiff M.D.'s birth control prescription, Defendant required Plaintiff M.D. to provide information regarding which birth control medications Plaintiff M.D. had used in the past and whether she was satisfied with them.

190. Once finished, Defendant would send medication to Plaintiff A.W.'s nearest pharmacy.

191. While Plaintiff A.W. was a user of Defendant's services, she never consented to or authorized the use of her Private Information by third parties or to Defendant enabling third parties to access, interpret, and use such Private Information.

192. Plaintiff A.W. 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.

193. After providing her Private Information to Defendant through the Website, Plaintiff A.W. immediately began seeing health ads targeted to her health conditions disclosed to Defendant as she scrolled through her accounts.

194. For example, Plaintiff A.W. received targeted ads, including but not limited to primary care options and medical insurance alternatives.

TOLLING

195. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know—and had no way of knowing—that their Private Information was intercepted and unlawfully disclosed to the Pixel Information Recipients because WISP kept this information secret.

CLASS ALLEGATIONS

196. 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).

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

> All persons residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the use of tracking technologies on Defendant's Website.

198. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff A.W. asserts claims on behalf of a North Carolina Subclass defined as:

> All persons residing in the State of North Carolina whose Private Information was disclosed to a third party without authorization or consent through the use of tracking technologies on Defendant's Website.

199. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff K.S.B. asserts claims on behalf of an Arkansas Subclass defined as:

> All persons residing in the State of Arkansas whose Private Information was disclosed to a third party without authorization or consent through the use of tracking technologies on Defendant's Website.

200. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff M.D. asserts claims on behalf of a District of Columbia Subclass defined as:

> All persons residing in the District of Columbia whose Private Information was disclosed to a third party without authorization or consent through the use of tracking technologies on Defendant's Website.

201. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff B.C. asserts claims on behalf of a Tennessee Subclass defined as:

> All persons residing in the State of Tennessee whose Private Information was disclosed to a third party without authorization or consent through the use of tracking technologies on Defendant's Website.

202. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff A.F. asserts claims on behalf of a Virginia Subclass defined as:

> All persons residing in the State of Virginia whose Private Information was disclosed to a third party without authorization or consent through the use of tracking technologies on Defendant's Website.

203. Excluded from the proposed Class and the Subclasses are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

204. 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.

205. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. On information and good faith belief, there are at least one million patients 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.

206. **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 their 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 patients' 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 their 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.

207. **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.

208. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek 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 have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

209. **Predominance**. Defendant have 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.

210. **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.

211. 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.

212. 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.

CALIFORNIA LAW APPLIES TO ALL CLAIMS ASSERTED IN THIS NATIONWIDE CLASS ACTION LAWSUIT

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

214. California, which seeks to protect the rights and interests of California and all residents and citizens of the United States against a company headquartered and doing business in California, has a greater interest in the claims of Plaintiffs and the

Class than any other state and is most intimately concerned with the claims and outcome of this litigation.

215. The principal place of business and headquarters of WISP, located at 548 Market Street in San Francisco, California, is the "nerve center" of its business activities—the place where its high-level officers direct, control and coordinate Defendant's activities, including major policy decisions.

216. Defendant's actions and corporate decisions surrounding the allegations made in the Complaint were made from and in San Francisco County, California. Moreover, Defendant's breaches of duty to Plaintiffs and Class members emanated from California.

217. Application of California law to the Class with respect to Plaintiffs' and Class members' claims is neither arbitrary nor fundamentally unfair because California has significant contacts and a significant aggregation of contacts that create a state interest in the common law claims of Plaintiffs and the Class.

218. Under California's choice of law principles, which are applicable to this action, the common law of California applies to the nationwide common law claims of all Class members.

219. Additionally, given California's significant interest in regulating the conduct of businesses operating within its borders, and that California has the most significant relationship to Defendant, as it is headquartered in California, and its executives and officers are located and made decisions which have given rise to the allegations and claims asserted herein, in California, there is no conflict in applying California law to non-resident consumers such as Plaintiffs and some of the potential Class members.

CAUSES OF ACTION

COUNT I

NEGLIGENCE
(*On behalf of Plaintiffs & the Nationwide Class*)

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

221. Upon accepting, storing, and controlling the Private Information of Plaintiffs and the Class, Defendant owed, and continues to owe, a duty to Plaintiffs and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information.

222. Defendant breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

223. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information through its use of the Pixels, Conversions API, and other tracking technologies would result in unauthorized third parties, such as the Pixel Information Recipients, gaining access to such Private Information for no lawful purpose.

224. Defendant's duty of care to use reasonable measures to secure and safeguard Plaintiffs' and Class Members' Private Information arose due to the special relationship that existed between Defendant and its Users, which is recognized by statute, regulations, and the common law.

225. In addition, Defendant had a duty under Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for but to any entity that may have access to healthcare

information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

226. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their Private Information. Defendant's misconduct included the failure to (1) secure Plaintiffs' and Class Members' Private Information; (2) comply with industry-standard data security practices; (3) implement adequate website and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Pixels, Conversions API, and other tracking technologies.

227. As a direct result of Defendant's breach of their duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class Members' Private Information, Plaintiffs and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

228. Defendant's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiffs' and Class Members' Private Information constituted (and continue to constitute) negligence at common law.

229. Plaintiffs and the Class are entitled to recover damages in an amount to be determined at trial.

COUNT II

INVASION OF PRIVACY—INTRUSION UPON SECLUSION

(On behalf of Plaintiffs & the Nationwide Class)

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

231. The highly sensitive and personal Private Information of Plaintiffs and Class Members consists of private and confidential facts and information regarding

Plaintiffs' and Class Members' health that were never intended to be shared beyond private communications on the Website and the consideration of health professionals.

232. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this Information against disclosure to unauthorized third parties, including the Pixel Information Recipients.

233. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

234. Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Private Information to the Pixel Information Recipients, third-party tech and marketing giants, is highly offensive to a reasonable person.

235. Defendant's willful and intentional disclosure of Plaintiffs' and Class Members' Private Information constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude and/or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

236. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiffs' and Class Members' privacy because Defendant facilitated the Pixel Information Recipients' simultaneous eavesdropping and wiretapping of confidential communications.

237. Defendant failed to protect Plaintiffs' and Class Members' Private Information and acted knowingly when it installed the Pixels onto the Website because the purpose of the Pixels is to track and disseminate an individual's communications on the Website for the purpose of marketing and advertising.

238. Because Defendant intentionally and willfully incorporated the Pixels into the Website and encouraged individuals to use and interact with the Website and the health services thereon, Defendant had notice and knew that their practices would cause injury to Plaintiffs and the Class.

239. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information, including the IIHI and PHI of Plaintiffs and Class Members, was disclosed to unauthorized third parties, causing Plaintiffs and the Class to suffer damages.

240. Plaintiffs, on behalf of themself and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, lost benefit of the bargain, plus pre-judgment interest and costs.

241. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information is still maintained by Defendant and still in the possession of the Pixel Information Recipients, and the wrongful disclosure of the Private Information cannot be undone.

242. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's and unauthorized third parties' continued possession of their sensitive and confidential Private Information. A judgment for monetary damages will not undo Defendant's disclosure of the Private Information to unauthorized third parties who, upon information and belief, continue to possess and utilize the Private Information.

243. Plaintiffs, on behalf of themself and Class Members, further seek injunctive relief to enjoin Defendant from intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT III

BREACH OF CONFIDENCE

(On behalf of Plaintiffs & the Nationwide Class)

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

245. Possessors of non-public medical information, such as Defendant, have a duty to keep such medical information completely confidential.

246. Plaintiffs and Class Members had reasonable expectations of privacy in the responses and communications entrusted to Defendant through their Website, which included highly sensitive Private Information.

247. Contrary to its duties as a telehealth institution and its express promises of confidentiality, Defendant installed the Pixels and Conversions API to disclose and transmit to third parties Plaintiffs' and Class Members' Private Information, including data relating to Plaintiffs' and Class Members' health.

248. These disclosures were made without Plaintiffs' or Class Members' knowledge, consent, or authorization.

249. The third-party recipients included, but may not be limited to, the Pixel Information Recipients.

250. As a direct and proximate cause of Defendant's unauthorized disclosures of Plaintiffs' and Class Members' Private Information, Plaintiffs and Class Members were damaged by Defendant's breach of confidentiality 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 health services that Plaintiffs and Class Members participated in; (d) general damages for invasion of their rights in an amount to be determined by a jury at trial; (e) nominal damages for each independent violation; (f) the unauthorized use of something of value (the highly sensitive Private Information) that belonged to Plaintiffs and Class Members and the obtaining of a benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation to Plaintiffs or Class Members for the unauthorized use of such data; (g) diminishment of the value of Plaintiffs' and Class Members' Private Information; and

(h) violation of property rights Plaintiffs and Class Members have in their Private Information.

COUNT IV

UNJUST ENRICHMENT

(On behalf of Plaintiffs & the Nationwide Class)

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

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

253. 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.

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

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

256. The benefits that Defendant derived from Plaintiffs and Class Members were not offered by Plaintiffs or Class Members gratuitously and, thus, rightly belong to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles in every state 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.

257. 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 V

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs & the Nationwide Class)

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

259. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for services, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

260. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

261. Plaintiffs and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

262. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information to third parties like Facebook.

263. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein.

264. Plaintiffs and Class Members would not have used Defendant's services or would have paid substantially for these services had they known their Private Information would be disclosed.

265. Plaintiffs and Class Members are entitled to compensatory, consequential, and/or nominal damages as a result of Defendant's breaches of implied contract.

COUNT VI

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT 18 U.S.C. § 2511(1), *et seq.*

(*On behalf of Plaintiffs & the Nationwide Class*)

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

267. The ECPA protects both sent and received communications.

268. 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.

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

270. The transmission of Private Information between Plaintiffs and Class Members and Defendant via its 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).

271. 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).

272. 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).

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

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's web servers and

d. The Pixels deployed by Defendant to effectuate the sending and acquisition of Users' sensitive communications.

274. By utilizing and embedding the Pixels and Conversions API on its 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).

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

276. 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 treatment plans in which Plaintiffs and Class Members participated.

277. 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).

278. 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).

279. 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.

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

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

282. 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 and Conversions API.

283. Any purported consent that Defendant received from Plaintiffs and Class Members was invalid.

284. 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.

COUNT VII

VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Cal. Civ. Code § 56, *et seq.*

(On behalf of Plaintiffs & the Nationwide Class)

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

286. Defendant is subject to the CMIA pursuant to California Civil Code § 56.10 because it is a "provider of health care" as defined by California Civil Code § 56.06(b); it operates hospitals, provides health care, maintains medical information, offers software to consumers designed to maintain medical information for the purposes of communications with doctors, receipt of diagnosis, treatment, or management of medical conditions.

287. Section 56.10 states, in pertinent part, that "[n]o provider of health care . . . shall disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization . . . ."

288. Section 56.101 of the CMIA states, in pertinent part, that "[a]ny provider of health care . . . who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties . . ." Cal. Civ. Code §§ 56.10, 56.101.

289. Plaintiffs' and Class Members' Private Information constitutes "medical information" under the CMIA because it consists of individually identifiable information in possession of and derived from a provider of healthcare regarding Plaintiffs' and Class Members' medical history, test results, mental or physical condition and/or treatment.

290. Defendant violated Cal. Civ. Code § 56.10 because it failed to maintain the confidentiality of Users' medical information, and instead "disclose[d] medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization" by soliciting,

intercepting and receiving Plaintiffs' and Class Members' Private Information, and sharing it with advertisers and for advertising purposes. Specifically, Defendant knowingly, willfully, or negligently disclosed Plaintiffs' and Class Members' medical information to Facebook, allowing Facebook to now advertise and target Plaintiffs and Class Members, misusing their extremely sensitive Private Information.

291. Defendant violated Cal. Civ. Code § 56.101 because they knowingly, willfully, or negligently failed to create, maintain, preserve, store, abandon, destroy and dispose of medical information in a manner that preserved its confidentiality by soliciting, intercepting, and receiving Plaintiffs' and Class Members' Private Information, and sharing it with advertisers and for advertising purposes for Facebook's and Defendant's financial gain.

292. Defendant intentionally embedded Facebook Pixels, which facilitate the unauthorized sharing of Plaintiffs' and Class Members' medical information.

293. Defendant violated Cal Civ. Code § 56.36(b) because they negligently released confidential information and records concerning Plaintiffs and Class Members in violation of their rights under the CMIA.

294. As a direct and proximate result of Defendant's misconduct, Plaintiffs and Class Members had their private communications containing information related to their sensitive and confidential Private Information intercepted, disclosed and used by third parties.

295. As a result of Defendant's unlawful conduct, Plaintiffs and Class Members suffered an injury, including violation to their rights of privacy, loss of the privacy of their Private Information, loss of control over their sensitive personal information, and suffered aggravation, inconvenience and emotional distress.

296. Plaintiffs and Class Members are entitled to: (a) nominal damages of $1,000 per violation; (b) actual damages, in an amount to be determined at trial; (c) reasonable attorneys' fees, and costs.

COUNT VIII

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT
Cal. Penal Code § 630, *et seq.*
(On behalf of Plaintiffs & the Nationwide Class)

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

298. 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 plaintiff 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.

299. 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).

300. Each of the Pixels and Conversions API is a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

301. At all relevant times, by employing the Pixels and Conversions API, 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.

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

303. 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.

304. 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 they frequently use the internet to search for information about products or services. They continue 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 have no practical way to know if their website communications will be monitored or recorded by the Pixel Information Recipients.

305. 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.

COUNT IX

VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT, Cal. Civ. Code § 1750, *et seq*.

(*On behalf of Plaintiffs & the Nationwide Class*)

306. Plaintiffs re-allege and incorporate the foregoing allegations above as if fully set forth herein.

307. Defendant engages in "unfair methods of competition and unfair or deceptive acts . . . in a transaction . . . that result[ed] . . . in the sale . . . of goods" to Plaintiffs and the Class Members in violation of Cal. Civ. Code § 1750 and Cal. Civ. Code § 1770(a)(5), (7), (9), (14), (16).

308. For instance, Defendant made representations that it would protect Plaintiffs' and the Class Members' privacy interest, including promising that it will keep Private Information private and secure, that Defendant does not sell Users' Private Information, and that it will only disclose Private Information under certain circumstances, none of which was true.

309. Defendant made these representations with no intention of living up to these representations. Contrary to these representations, Defendant disclosed and allowed third parties to intercept its customers' Private Information.

310. Further, Defendant failed to disclose it secretly shared, used, and allowed third parties to intercept Plaintiffs' and Class Members' Private Information.

311. Defendant was under a duty to disclose this information given Defendant's relationship with its customers and Defendant's exclusive knowledge of its misconduct (e.g., the tracking technology incorporated on Defendant's Website, the fact that Private Information is disclosed to unauthorized third parties, that Defendant allowed third parties to intercept Private Information through this technology, and how Defendant and third parties used this data).

312. Plaintiffs and Class Members would not have purchased or would have paid significantly less for Defendant's services and products had Defendant not made these false representations. Defendant profited directly from these sales, including through payment for these services and products, and from the Private Information disclosed and intercepted.

313. Plaintiffs, individually and on behalf of the Class Members, seek an injunction requiring Defendant to obtain consent prior to disclosing and otherwise using Plaintiffs' and Class Members' Private Information and to delete the Private Information already collected and any other relief which the court deems proper.

314. Pursuant to Cal. Civ. Code § 1782(a), Plaintiffs will serve Defendant with notice of its alleged violations of the CLRA by certified mail return receipt requested contemporaneously with the filing of this complaint. Should Defendant fail to provide appropriate relief for its violations of the CLRA within 30 days, Plaintiffs intend to seek monetary damages under the CLRA.

COUNT X

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, *et seq*.
Unlawful and Fraudulent Business Practices
(On behalf of Plaintiffs & the Nationwide Class)

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

316. Plaintiffs, Class Members and Defendant are each a "person" under Cal. Bus. & Prof. Code § 17201.

317. The acts, omissions, and conduct of Defendant as alleged herein constitute "business practices" within the meaning of the UCL.

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

319. Plaintiffs bring their claims for injunctive relief as they have no confidence that Defendant has altered its privacy practices and they may wish to use Defendant's services in the future.

320. Plaintiffs bring their claims for restitution in the alternative to their claims for damages.

321. Defendant's business acts and practices are "unlawful" under the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et. seq*. because, as alleged above, Defendant violated California common law, the California Constitution, and other statutes and causes of action alleged herein.

322. Defendant engages in unlawful business practices by disclosing Plaintiffs' and Class Members' Private Information to unrelated third parties, including Facebook, by embedding the Pixel on its Website without prior consent in violation of the consumer protection and privacy statutes alleged herein, including the following: California Constitution, Article I, section 1; Cal. Penal Code §§ 630, *et. seq.*; Cal. Civ. Code §§ 56, *et. seq.*; 18 U.S.C. § 2511(1), *et seq.*; 18 U.S.C. § 2511(3)(a), *et seq.*; Section 5 of the FTC Act, 15 U.S.C 45, et seq.; and the HIPAA violations set forth above.

323. Because Defendant is in the business of providing healthcare services, Plaintiff and Class Members relied on Defendant to advise them of any potential disclosure of their Private Information. Plaintiff and Class Members understood that Defendant, as a healthcare provider, would take appropriate measures to keep their Private Information private and confidential.

324. In its privacy policies, Defendant promised that it would not share Plaintiffs' and Class Members' Private Information with any third party without consent or for marketing purposes. Contrary to its own policies, Defendant did disclose Plaintiffs' and Class Members' Private Information to third parties without consent and for marketing purposes.

325. Had Defendant disclosed that it shared Private Information with third parties, Plaintiffs would have been aware of the disclosure and would not have used Defendant's services or would have paid considerably less for those services.

326. As a direct and proximate result of Defendant's violations of the UCL, Plaintiffs and Class Members have suffered injury in fact and lost money or property, including, but not limited to, payments Plaintiffs and Class Members made to Defendant and/or other valuable consideration, in addition to the exposure of their Private Information. Plaintiffs and Class Members also lost the value of their Private Information because of Defendant's unlawful disclosures.

327. Plaintiffs and Class Members also face a real and immediate threat of future injury to the confidentiality of their Private Information because such information remains within Defendant's control and because anytime that Plaintiffs and Class Members interact with the Website to submit information about their medical conditions, search for treatments including specific medications, or otherwise seek assistance related to their medical conditions, Plaintiffs and Class Members risk further disclosure of their Private Information. Plaintiffs continue to want to use Defendant's Website and would resume using Wisp's services if Defendant complies with applicable laws and stops using the Pixel on its Website. Plaintiffs and Class Members are, therefore, entitled to injunctive relief, requiring that Defendant cease all website operations that allow for the third-party capture of Private Health Information.

328. As a direct result of its unlawful and deceptive practices, Defendant has been unjustly enriched and should be required to make restitution to Plaintiffs and t Class Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code, restitutionary disgorgement of all profits accruing to Defendant because of its unlawful business practices, declaratory relief, attorney fees, and costs of litigation (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

329. In the alternative to those claims seeking remedies at law, Plaintiffs and Class Members allege that there is no plain, adequate, and complete remedy that exists at law to address Defendant's unlawful and unfair business practices.

330. The legal remedies available to Plaintiffs are inadequate because they are not "equally prompt and certain and in other ways efficient" as equitable relief. *American Life Ins. Co. v. Stewart*, 300 U.S. 203, 214 (1937); *see also United States v. Bluitt*, 815 F. Supp. 1314, 1317 (N.D. Cal. Oct. 6, 1992) ("The mere existence' of a possible legal remedy is not sufficient to warrant denial of equitable relief.").

331. Additionally, unlike damages, the Court's discretion in fashioning equitable relief is very broad and can be awarded in situations where the entitlement to damages may prove difficult. *Cortez v. Purolator Air Filtration Products Co.*, 23 Cal.4th 163, 177-180 (2000) (Restitution under the UCL can be awarded "even absent individualized proof that the claimant lacked knowledge of the overcharge when the transaction occurred.").

332. Thus, restitution would allow recovery even when normal consideration associated with damages would not. *See, e.g., Fladeboe v. Am. Isuzu Motors Inc.*, 150 Cal. App. 4th 42, 68 (2007) (noting that restitution is available even in situations where damages may not be available). Furthermore, the standard for a violation of the UCL "unlawful" prong is different from the standard that governs legal claims.

COUNT XI

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, *et seq.*
Unfair Business Practices
(On behalf of Plaintiffs & the Nationwide Class)

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

334. Defendant's business acts and practices meet the unfairness prong of the UCL according to all three theories of unfairness.

335. First, Defendant's business acts and practices are "unfair" under the UCL pursuant to the three-part test articulated in *Camacho v. Automobile Club of Southern California* (2006) 142 Cal. App. 4th 1394, 1403: (a) Plaintiffs and Class Members suffered substantial injury due to Defendant's disclosure of their Private Information; (b) Defendant's disclosure of Plaintiffs' and Class Members' Private Information provides no benefit to consumers, let alone any countervailing benefit that could justify Defendant's disclosure of Private Information without consent for marketing purposes or other pecuniary gain; and (c) Plaintiffs and Class Members could not have readily avoided this injury because they had no way of knowing that Defendant was implementing the Pixel. Thus, Plaintiffs and Class Members did not know to ask Defendant to stop the practice of disclosing their Private Information and did not know that they should stop using Defendant's services to avoid disclosing their Private Information

336. Second, Defendant's business acts and practices are "unfair" under the UCL because they are "immoral, unethical, oppressive, unscrupulous, or substantially injurious" to Plaintiffs and Class Members, and "the utility of [Defendant's] conduct," if any, does not "outweigh the gravity of the harm" to Plaintiffs and Class Members. *Drum v. San Fernando Valley Bar Ass'n*, (2010) 182 Cal. App. 4th 247, 257. Defendant engages in unfair business practices by disclosing Plaintiffs' and Class Members' Private Information to unrelated third parties, including Facebook, without prior consent despite its promises to keep such information confidential. This surreptitious and undisclosed conduct is immoral, unethical, oppressive, unscrupulous, and substantially injurious. No benefit inheres in this conduct, the gravity of which is significant.

337. Third, Defendant's business acts and practices are "unfair" under the UCL because they run afoul of "specific constitutional, statutory, or regulatory provisions." *Drum*, 182 Cal. App. 4th at 256 (internal quotation marks and citations omitted). California has a strong public policy of protecting consumers' privacy interests,

including consumers' and patients' personal data. This public policy is codified in California's Constitution in Article I, section 1; CIPA, Cal. Penal Code §§ 630, *et seq*.; the CMIA, Cal. Civil Code §§ 56.06, 56.10, 56.101; and the California Consumer Privacy Act, Cal. Civil Code §§ 1798, *et seq*., among other statutes.

338. This public policy is further codified on a nationwide basis in federal statutes, including HIPAA, the FTC Act, and the ECPA. Defendant violated this public policy by, among other things, surreptitiously collecting, disclosing, and otherwise exploiting Plaintiffs' and Class Members' Private Information by sharing it with Facebook and other third parties via the Pixel without Plaintiffs' and/or Class Members' consent.

339. Because Defendant is in the business of providing healthcare services, Plaintiffs and Class Members relied on Defendant to advise them of any potential disclosure of their Private Information.

340. Plaintiffs and Class Members understood that Defendant, as a healthcare provider, would take appropriate measures to keep their private information private and confidential.

341. In its privacy policies, Defendant promised that it would not share Plaintiffs' and Class Members' private information with any third party without consent or for marketing purposes. Contrary to its own policies, Defendant did disclose Plaintiffs' and Class Members' Private Information to third parties without consent and for marketing purposes. Defendant was in sole possession of and had a duty to disclose the material information that Plaintiffs' and Class Members' Private Information was being shared with a third party.

342. Had Defendant disclosed that it shared Private Information with third parties, Plaintiffs would not have used Defendant's services or would have paid considerably less for those services.

343. The harm caused by Defendant's conduct outweighs any potential benefits attributable to such conduct, and there were reasonably available alternatives to further

Defendant's legitimate business interests other than Defendant's conduct described herein.

344. Plaintiffs and Class Members trusted Defendant to keep their Private Information confidential, and as a result, shared highly sensitive information through their use of the Website, causing them to suffer damages when Defendant disclosed that information to a third party.

345. As a direct and proximate result of Defendant's violations of the UCL, Plaintiffs and Class Members have suffered injury in fact and lost money or property, including, but not limited to, payments Plaintiffs and Class Members made to Defendant and/or other valuable consideration, such as access to their private and personal data. Plaintiffs and Class Members also lost the value of their Private Information as a result of Defendant's unfair business practices.

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

347. In the alternative to those claims seeking remedies at law, Plaintiffs and Class Members allege that there is no plain, adequate, and complete remedy that exists at law to address Defendant's unlawful and unfair business practices. The legal remedies available to Plaintiff are inadequate because they are not "equally prompt and certain and in other ways efficient" as equitable relief. *American Life Ins. Co. v. Stewart*, 300 U.S. 203, 214 (1937); *see also United States v. Bluitt*, 815 F. Supp. 1314, 1317 (N.D. Cal. Oct. 6, 1992) ("The mere existence' of a possible legal remedy is not sufficient to warrant denial of equitable relief.").

348. Additionally, unlike damages, the Court's discretion in fashioning equitable relief is very broad and can be awarded in situations where the entitlement to

damages may prove difficult. *Cortez v. Purolator Air Filtration Products Co.*, 23 Cal.4th 163, 177-180 (2000) (Restitution under the UCL can be awarded "even absent individualized proof that the claimant lacked knowledge of the overcharge when the transaction occurred.").

349. Thus, restitution would allow recovery even when normal consideration associated with damages would not. *See, e.g., Fladeboe v. Am. Isuzu Motors Inc.*, 150 Cal. App. 4th 42, 68 (2007) (noting that restitution is available even in situations where damages may not be available). Furthermore, the standard for a violation of the UCL "unfair" prong is different from the standard that governs legal claims.

COUNT XII

VIOLATION OF NORTH CAROLINA'S UNFAIR & DECEPTIVE PRACTICES ACT N.C. Gen. Stat. § 75-1.1, *et seq*.

(Alternatively, and on behalf of Plaintiff A.W. & the North Carolina Subclass)

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

351. This count is pleaded in the alternative to all California specific claims above (Counts VII-X), in the event the Court finds that California law does not apply to Plaintiff A.W. and the North Carolina Subclass.

352. N.C. Gen. Stat. § 75-1.1. (the "NC UDTPA") declares unlawful "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."

353. Defendant's conduct was in and affecting commerce and constitutes an unfair or deceptive trade practice under the NC UDPTA.

354. Specifically, Defendant's unlawful disclosure of Plaintiff A.W.'s and the North Carolina Subclass Members' Private Information constitutes a per se violation of NC UDPTA.

355. Defendant engages in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the NC UDPTA by: (i) unlawfully disclosing Plaintiff A.W.'s and the North Carolina Subclass Members' Private Information to Facebook and other third parties; (ii) failing to disclose or omitting material facts to Plaintiff A.W. and the North Carolina Subclass Members regarding the disclosure of their Private Information to Facebook and other third parties; and (iii) failing to take proper action to ensure the proper pixel was configured to prevent unlawful disclosure of Plaintiffs A.W.'s and the North Carolina Subclass Members' Private Information.

356. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant knew it failed to disclose to Plaintiff A.W. and the North Carolina Subclass Members that their healthcare-related communications via the Website would be disclosed to Facebook and other third parties.

357. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant intended that Plaintiff A.W. and the North Carolina Subclass Members rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

358. Specifically, Defendant was aware that Plaintiff A.W. and the North Carolina Subclass Members depended on and relied upon it to keep their communications confidential. Instead, Defendant disclosed that information to Facebook and other unauthorized third parties without consent.

359. In addition, Defendant's material failure to disclose that Defendant collects Plaintiff A.W.'s and the North Carolina Subclass Members' Private Information for marketing purposes with Facebook constitutes an unfair act or practice prohibited by the NC UDPTA. Defendant's actions were immoral, unethical, and unscrupulous.

360. Plaintiff A.W. had a reasonable expectation of privacy in her communications exchanged with Defendant, including communications exchanged on Defendant's Website.

361. Plaintiff A.W.'s and the North Carolina Subclass Members' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its Notice of Privacy Practices.

362. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed pixel code to disclose and transmit Plaintiff A.W.'s and the North Carolina Subclass Members' personally identifiable, non-public medical information, and the contents of their communications exchanged with Defendant to third parties, including Facebook.

363. Defendant's disclosures of Plaintiff A.W.'s and the North Carolina Subclass Members' Private Information were made without their knowledge, consent, or authorization and were unprivileged.

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

365. Defendant willfully, knowingly, intentionally, and voluntarily engages in the aforementioned acts when it incorporated the Facebook Pixel with knowledge of the Pixel's purpose and functionality.

366. The harm described herein could not have been avoided by Plaintiff A.W. and the North Carolina Subclass Members through the exercise of ordinary diligence.

367. As a result of Defendant's wrongful conduct, Plaintiff A.W. was injured in that, she never would have provided her PII and PHI to Defendant or purchased Defendant's services had she known or been told that Defendant shared her confidential and sensitive Private Information with Facebook.

368. As a direct and proximate result of Defendant's violations of the NC UDPTA, Plaintiff A.W. and the North Carolina Subclass Member have suffered harm,

including financial losses related to the payments or services made to Defendant that Plaintiffs and the North Carolina Subclass Members would not have made had they known of Defendant's disclosure of their PII and PHI to Facebook; lost control over the value of their PII and PHI; and other harm resulting from the unauthorized use or threat of unauthorized use of their PII and PHI, including for unwanted solicitations or marketing, entitling them to damages in an amount to be proven at trial.

369. Pursuant to N.C. Gen. Stat. § 75-16, § 75.16.1, Plaintiff A.W. requests damages, treble damages, punitive damages, and attorneys' fees in addition to all other relief allowed by law.

COUNT XIII

VIOLATION OF THE ARKANSAS DECEPTIVE TRADE PRACTICES ACT
Ark. Code Ann § 4-88-101, *et seq.*
(Alternatively, and on behalf of Plaintiff K.S.B & the Arkansas Subclass)

370. Plaintiff K.S.B. re-alleges and incorporates by reference the allegations above as if fully set forth herein.

371. This count is pleaded in the alternative to all California specific claims above (Counts VII-X), in the event the Court finds that California law does not apply to Plaintiff K.S.B and the Arkansas Subclass.

372. Defendant's products and services are "goods" and "services" as defined by Ark. Code Ann. §§ 4-88-102(4) and (7).

373. Defendant advertised, offered or sold goods or services in Arkansas and engages in trade or commerce directly or indirectly affecting the people of Arkansas.

374. The Arkansas Deceptive Trade Practices Act ("ADTPA"), Ark. Code Ann. §§ 4-88-101, et seq., prohibits unfair, deceptive, false and unconscionable trade practices.

375. Specifically, Defendant's unlawful disclosure of Plaintiff K.S.B's and the Arkansas Subclass Members' Private Information constitutes a per se violation of the ADTPA.

376. Defendant engages in acts of deception and false pretense in connection with the sale and advertisement of services in violation of Ark. Code Ann. § 4-88-1-8(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of Ark. Code Ann. § 4-88-1-8(2), and engages in the following deceptive trade practices defined in Ark. Code Ann. § 4-88-107: (i) unlawfully disclosing Plaintiff K.S.B's and the Arkansas Subclass Members' Private Information to Facebook and other third parties; (ii) failing to disclose or omitting material facts to Plaintiff K.S.B and the Arkansas Subclass Members regarding the disclosure of their Private Information to Facebook and other third parties; and (iii) failing to take proper action to ensure the proper pixel was configured to prevent unlawful disclosure of Plaintiff K.S.B's and the Arkansas Subclass Members' Private Information.

377. Defendant's actions also constitute unconscionable, false and deceptive practices because Defendant knew it failed to disclose to Plaintiff K.S.B and the Arkansas Subclass Members that their healthcare-related communications via the Website would be disclosed to Facebook and other third parties.

378. Defendant's actions also constitute unconscionable, false and deceptive practices because Defendant intended that Plaintiff K.S.B and the Arkansas Subclass Members rely on its deceptive practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

379. Specifically, Defendant was aware that Plaintiff K.S.B and the Arkansas Subclass Members depended on and relied upon it to keep their communications confidential. Instead, Defendant disclosed that information to Facebook and other unauthorized third parties without consent.

380. Defendant omitted, suppressed and concealed the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff K.S.B's and the Arkansas Subclass Members's Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

381. Plaintiff K.S.B had a reasonable expectation of privacy in its communications exchanged with Defendant, including communications exchanged on Defendant's Website.

382. Plaintiff K.S.B's and the Arkansas Subclass Members's reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its Notice of Privacy Practices.

383. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed pixel code to disclose and transmit Plaintiff K.S.B's and the Arkansas Subclass Members's personally identifiable, non-public medical information, and the contents of their communications exchanged with Defendant to third parties, including Facebook.

384. Defendant's disclosures of Plaintiff K.S.B's and the Arkansas Subclass Members's Private Information were made without their knowledge, consent, or authorization and were unprivileged.

385. As a result, 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' PII and PHI.

386. Defendant intended to mislead Plaintiff K.S.B and the Arkansas Subclass Members and induce them to rely on its misrepresentations and omissions.

387. As a result of Defendant's wrongful conduct, Plaintiff K.S.B and the Arkansas Subclass Members were injured in that, they never would have provided their PII and PHI to Defendant or purchased Defendant's services had they known or been

told that Defendant shared their confidential and sensitive Private Information with Facebook.

388. Defendant acted intentionally, knowingly and maliciously to violate the ADTPA, and recklessly disregarded Plaintiff K.S.B and the Arkansas Subclass Members's rights.

389. As a direct and proximate result of Defendant's unconscionable, unfair and deceptive acts or practices in violation of the ADTPA, Plaintiff K.S.B and the Arkansas Subclass Members have suffered harm, including financial losses related to the payments or services made to Defendant that Plaintiff and the Arkansas Subclass Members would not have made had they known of Defendant's disclosure of their PII and PHI to Facebook; lost control over the value of their PII and PHI; and other harm resulting from the unauthorized use or threat of unauthorized use of their PII and PHI, including for unwanted solicitations or marketing, entitling them to damages in an amount to be proven at trial.

390. Plaintiff K.S.B and the Arkansas Subclass Members seek all monetary and non-monetary relief allowed by law, including actual financial losses, injunctive relief and reasonable attorneys' fees and costs.

COUNT XIV

VIOLATION OF THE DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT D.C. Code § 28-3901, *et seq.*

(Alternatively, and on behalf of Plaintiff M.D. & the District of Columbia Subclass)

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

392. This count is pleaded in the alternative to all California specific claims above (Counts VII-X), in the event the Court finds that California law does not apply to Plaintiff M.D. and the District of Columbia Subclass.

393. Defendant engages in unfair competition or unfair, unconscionable, deceptive or fraudulent acts or practices in violation of the District of Columbia Consumer Protection Procedures Act, D.C. Code Ann. § 28-3901 *et seq.*, when it misled consumers and failed to disclose to Plaintiff M.D. and the District of Columbia Subclass Members that their healthcare-related communications via the Website would be disclosed to Facebook and other third parties.

394. As a direct result of Defendant's deceptive, unfair, unconscionable and fraudulent conduct, Plaintiff M.D. and the District of Columbia Subclass Members suffered and will continue to suffer economic loss and other compensable injuries.

395. Defendants' deceptive, unfair, unlawful and unconscionable practices included but were not limited to the following practices, done knowingly:

a. Representing that goods or services have characteristics, ingredients, uses or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade if they are of another; and

c. Advertising goods or services with the intent not to sell them as advertised.

396. Defendant's actions and failures to act—including its false and misleading representations and omissions of material facts regarding the disclosure of Plaintiff M.D.'s and the District of Columbia Subclass Members' Private Information, as described above—constitute acts, uses or employment by Defendant of unconscionable commercial practices, deception, fraud, false pretenses and misrepresentations. These actions and omissions further constitute the knowing concealment, suppression or omission of material facts, done with the intent that Plaintiff M.D. and the District of Columbia Subclass Members rely upon such concealment, suppression or omission of material facts in connection with the sale of Defendant's services, in violation of the District of Columbia Consumer Protection Procedures Act.

397. Defendant's unfair and deceptive trade practices have caused injuries to consumers, and the public will benefit from a cessation of these unlawful actions through this litigation.

398. By reason of the unlawful acts engaged in by Defendant, Plaintiff M.D. and the District of Columbia Subclass Members have suffered ascertainable loss and damages.

399. As a direct and proximate result of Plaintiff M.D.'s and the other District of Columbia Subclass Members' reasonably anticipated use of Defendant's Website as manufactured, designed, sold, supplied, marketed and/or introduced into the stream of commerce by Defendant, Plaintiff M.D. and the other District of Columbia Subclass Members suffered serious injury, harm, damages, economic and non-economic loss and will continue to suffer such harm, damages and losses in the future.

400. Defendant's conduct indicates a wanton disregard of the rights of others, justifying an award of punitive or exemplary damages. Due to the above, Defendant is liable to Plaintiff M.D. and the other District of Columbia Subclass Members for compensatory, as well as exemplary, multiple and/or punitive damages to the extent available and as applicable, in amounts to be proven at trial, together with interest, costs of suit, attorneys' fees and all such other relief as the Court deems proper.

401. Plaintiff M.D. did not need to send (additional) notice to Defendant of its violations of the District of Columbia Consumer Protection Procedures Act pled in this Complaint because Defendant was already on notice of the defects alleged herein. Defendant received such notice from similar lawsuits for the same conduct and through other means, including media reporting, HHS Guidance and FTC policies.

402. Plaintiff M.D. and the other District of Columbia Subclass Members would not have used Defendant's Website and services, or alternatively they would have paid less for them, had the truth about the nature of Defendant's products and services been disclosed.

403. Plaintiff and the other District of Columbia Subclass Member seek all monetary and non-monetary relief allowed by law, including actual financial losses, injunctive relief and reasonable attorneys' fees and costs.

COUNT XV

VIOLATION OF THE TENNESSEE TRADE PRACTICES ACT
Tennessee Code Annotated § 47-25-101, *et seq.*
(Alternatively, and on behalf of Plaintiff B.C & the Tennessee Subclass)

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

405. This count is pleaded in the alternative to all California specific claims above (Counts VII-X), in the event the Court finds that California law does not apply to Plaintiff B.C and the Tennessee Subclass.

406. Defendant engages in unfair competition or unfair, unconscionable, deceptive or fraudulent acts or practices in violation of the Tennessee Consumer Protection Act, Tenn. Code Ann. § 47-25-101 *et seq.*, when it misled consumers by embedding the Pixel on its Website without prior consent in violation of the consumer protection and privacy statutes alleged herein. As a direct result of Defendant's deceptive, unfair, unconscionable and fraudulent conduct, Plaintiff B.C and the other Tennessee Subclass Members suffered and will continue to suffer economic loss and other compensable injuries.

407. Defendant's deceptive, unfair, unlawful and unconscionable practices include but were not limited to the following practices, done knowingly:

a. Representing that goods or services have characteristics, ingredients, uses or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade if they are of another; and

c. Advertising goods or services with the intent not to sell them as advertised.

408. Defendant's actions and failure to act—including its false and misleading representations and omissions of material facts regarding its disclosure of Private Information via tracking pixels on its Website, as described above—constitute acts, uses or employment by Defendant of unconscionable commercial practices, deception, fraud, false pretenses and misrepresentations. These actions and omissions further constitute the knowing concealment, suppression or omission of material facts, done with the intent that Plaintiff B.C and the other Tennessee Subclass Members rely upon such concealment, suppression or omission of material facts in connection with the sale of Defendant's merchandise and services, in violation of the Tennessee Consumer Protection Act.

409. Defendant's unfair and deceptive trade practices have caused injuries to consumers, and the public will benefit from a cessation of these unlawful actions through this litigation.

410. By reason of the unlawful acts engaged in by Defendant, Plaintiff B.C and the other Tennessee Subclass Members have suffered ascertainable loss and damages.

411. As a direct and proximate result of Plaintiff B.C's and the other Tennessee Subclass Members' reasonably anticipated use of Defendant's Website and services as manufactured, designed, sold, supplied, marketed and/or introduced into the stream of commerce by Defendant, Plaintiff and the other Tennessee Subclass Members suffered serious injury, harm, damages, economic and non-economic loss and will continue to suffer such harm, damages and losses in the future.

412. Defendant's conduct with respect to its design and sale of its Website and services to Plaintiff B.C and the other Tennessee Subclass Members was fraudulent, malicious, oppressive, willful, reckless and/or grossly negligent, and Defendant's conduct indicates a wanton disregard of the rights of others, justifying an award of punitive or exemplary damages.

413. Due to the above, Defendant is liable to Plaintiff B.C and the other Tennessee Subclass Members for compensatory, as well as exemplary, multiple, and/or

punitive damages to the extent available and as applicable, in amounts to be proven at trial, together with interest, costs of suit, attorneys' fees and all such other relief as the Court deems proper.

414. Plaintiff did not need to send (additional) notice to Defendant of its violations of the Tennessee Consumer Protection Act pled in this Complaint because Defendant was already on notice of the defects alleged herein. Defendant received such notice from similar lawsuits for the same conduct and through other means, including media reporting, HHS Guidance and FTC policies.

415. Plaintiff B.C and the other Tennessee Subclass Members would not have used Defendant's Website or services, or alternatively they would have paid less for them, had the truth about the nature of Defendant's products or services been disclosed.

416. Plaintiff and the other Tennessee Subclass Members seek all monetary and non-monetary relief allowed by law, including actual financial losses, injunctive relief and reasonable attorneys' fees and costs.

COUNT XVI

VIOLATION OF THE VIRGINIA CONSUMER PROTECTION ACT
Virginia Code Ann. § 59.1-196, *et seq.*
(Alternatively, and on behalf of Plaintiff A.F. & the Virginia Subclass)

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

418. This count is pleaded in the alternative to all California specific claims above (Counts VII-X), in the event the Court finds that California law does not apply to Plaintiff A.F. and the Virginia Subclass.

419. Defendant engages in unfair competition or unfair, unconscionable, deceptive or fraudulent acts or practices in violation of the Virginia Consumer Protection Act, Va. Code Ann. § 59.1-196 *et seq.*, when it misled consumers by embedding the Pixel on its Website without prior consent in violation of the consumer

protection and privacy statutes alleged herein. As a direct result of Defendant's deceptive, unfair, unconscionable and fraudulent conduct, Plaintiff A.F. and the other Virginia Subclass Members suffered and will continue to suffer economic loss and other compensable injuries.

420. Defendant's deceptive, unfair, unlawful and unconscionable practices include but were not limited to the following practices, done knowingly:

a. Representing that goods or services have characteristics, ingredients, uses or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade if they are of another; and

c. Advertising goods or services with the intent not to sell them as advertised.

421. Defendant's actions and failure to act—including its false and misleading representations and omissions of material facts regarding its disclosure of Private Information via tracking pixels on its Website, as described above—constitute acts, uses or employment by Defendant of unconscionable commercial practices, deception, fraud, false pretenses and misrepresentations. These actions and omissions further constitute the knowing concealment, suppression or omission of material facts, done with the intent that Plaintiff A.F. and the other Virginia Subclass Members rely upon such concealment, suppression or omission of material facts in connection with the sale of Defendant's merchandise and services, in violation of the Virginia Consumer Protection Act.

422. Defendant's unfair and deceptive trade practices have caused injuries to consumers, and the public will benefit from a cessation of these unlawful actions through this litigation.

423. By reason of the unlawful acts engaged in by Defendant, Plaintiff A.F. and the other Virginia Subclass Members have suffered ascertainable loss and damages.

424. As a direct and proximate result of Plaintiff A.F.'s and the other Virginia Subclass Members' reasonably anticipated use of Defendant's Website and services as

manufactured, designed, sold, supplied, marketed and/or introduced into the stream of commerce by Defendant, Plaintiff and the other Virginia Subclass Members suffered serious injury, harm, damages, economic and non-economic loss and will continue to suffer such harm, damages and losses in the future.

425. Defendant's conduct with respect to its design and sale of its Website and services to Plaintiff A.F. and the other Virginia Subclass Members was fraudulent, malicious, oppressive, willful, reckless and/or grossly negligent, and Defendant's conduct indicates a wanton disregard of the rights of others, justifying an award of punitive or exemplary damages.

426. Due to the above, Defendant is liable to Plaintiff A.F. and the other Virginia Subclass Members for compensatory, as well as exemplary, multiple, and/or punitive damages to the extent available and as applicable, in amounts to be proven at trial, together with interest, costs of suit, attorneys' fees and all such other relief as the Court deems proper.

427. Plaintiff did not need to send (additional) notice to Defendant of its violations of the Virginia Consumer Protection Act pled in this Complaint because Defendant was already on notice of the defects alleged herein. Defendant received such notice from similar lawsuits for the same conduct and through other means, including media reporting, HHS Guidance and FTC policies.

428. Plaintiff A.F. and the other Virginia Subclass Members would not have used Defendant's Website or services, or alternatively they would have paid less for them, had the truth about the nature of Defendant's products or services been disclosed.

429. Plaintiff and the other Virginia Subclass Members seek all monetary and non-monetary relief allowed by law, including actual financial losses, injunctive relief and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class and the Subclasses, respectfully request that this Court enter an Order:

a) Certifying this case as a class action on behalf of the Nationwide Class defined above, appointing Plaintiffs as representatives of the Class, and appointing their counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or unauthorized disclosure of Plaintiffs' and Class Members' Private Information;

c) For 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) For an award of damages including, but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

e) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

f) Pre- and post-judgment interest on any amounts awarded and

g) Such other and further relief as this court may deem just and proper.

Dated: November 28, 2023

Respectfully submitted,

ALMEIDA LAW GROUP LLC

/s/ John R. Parker, Jr.

David S. Almeida*
Britany A. Kabakov*
Matthew J. Langley
John R. Parker, Jr.
3550 Watt Avenue, Suite 140
Sacramento, California 95821
(916) 616-2936

david@almeidalawgroup.com
britany@almeidalawgroup.com
matt@almeidalawgroup.com
jrparker@almeidalawgroup.com

MIGLIACCIO & RATHOD, LLP

/s/ Nichola Migliaccio
Nicholas Migliaccio*
412 H St. NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730
nmigliaccio@classlawdc.com

**pro hac vice anticipated*

Attorneys for Plaintiffs & the Classes