UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS

ASHLEY REEDY, JOSHUA COOK, MELODY SCHOON, JASMINE SMITH AND SHADARI BUSH, *individually and on behalf of all others similarly situated*,	)	**Case No.**
v.	)	**JURY TRIAL DEMANDED**
EVERLYWELL, INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiffs Ashley Reedy, Joshua Cook, Melody Schoon, Jasmine Smith and Shadari Bush ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through undersigned counsel, hereby allege the following against Everly Well, Inc., d/b/a Everlywell and Everly Health, a Delaware corporation ("Everlywell" 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 on due investigation of counsel and upon information and good faith belief.

NATURE OF THE ACTION

1. Defendant is a digital health testing company that offers customers over 30 at-home lab tests for purchase in 49 states, including Illinois, for a variety of medical conditions including highly sensitive sexual health conditions, with some tests costing as much as $299.[1]

[1] *See* https://www.everlywell.com/blog/news-and-info/where-to-buy-everlywell-tests/; *see also* https://www.everlywell.com/products/ (last accessed Mar. 9, 2024). In addition to selling its test kits online, Everlywell also distributes them via brick-and-mortar stores including CVS, Kroger,

2. Everlywell boldly proclaims on its "Notice of Privacy Practices" the lengths it will supposedly go to protect its customers' personal health information:

> "***[u]nder no circumstance do we ever sell our customers' data***, and we use state-of-the-art, bank-grade encryption to ensure data security. ***Customer information is only shared with the labs and physicians that are part of our testing process. Everlywell's best-in-class, secure handling of personal health information earned the company "Highly Compliant" status per the HIPAA/HITECH Security Standards***."[2]

3. As detailed herein, those statements are certainly suspect given Defendant's outrageous, illegal and widespread practice of disclosing Plaintiffs' and putative Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (referred to herein collectively as "Private Information") to third parties, including, but not necessarily limited to, Meta Platforms, Inc. d/b/a Meta ("Facebook") and Google LLC ("Google").

4. 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.[3]

Target, and Walgreens. *Id*.

[2] *See Consumer Protections*, https://www.everlywell.com/blog/news-and-info/where-to-buy-everlywell-tests/ (emphasis added) (last accessed Mar. 9, 2024).

[3] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world* (Nov. 16, 2022), available at https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited Mar. 9, 2024) ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized."); *see also* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites* (June 16, 2022), available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited Mar. 9, 2024).

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

6. Reiterating the importance of and necessity for data security and privacy concerning health information, the Federal Trade Commission ("FTC") recently published a bulletin entitled *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases*, in which it noted that "[h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer's health***. Indeed, [recent FTC enforcement actions involving] *Premom*, *BetterHelp*, *GoodRx* and *Flo Health* ***make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or fertility, for example—or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information."***[4]

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

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

[4] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases* (July 25, 2023) (emphasis added), available at https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Mar. 9, 2024).

> 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***.[5]

8. The incontrovertible need for data security and transparency is particularly acute when it comes to the rapidly expanding worlds of telehealth and diagnostic test kits delivered to consumers' homes.

9. Garnering wide-spread adaptation during the COVID-19 pandemic, these self-collection or at-home testing kits form an important part of consumers' access to healthcare by removing the impediments of having to travel to visit with medical providers – not to mention that these kits allow for quick turnaround at often cheaper price points, in the (supposed) privacy of their own home.

10. Despite these kits testing for extremely sensitive and personal issues like sexual and reproductive health, many of these at-home test kit retailers appear to value the collection and monetization of user data over all else.[6] And, the universe of data that these companies collect is

---

[5] *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.

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

extremely vast as at-home test providers (and the laboratories with which they partner) can collect personal and health data on their customers through several channels, including through an initial online symptom survey, purchase information, customer interactions with provider websites or apps, and test results.[7]

11. Unfortunately, the process of searching for, researching, purchasing and using these kits is ***not*** as confidential a process as the retailers of these kits make it seem.

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

13. That investigation found that "trackers collecting browsing- and purchase-related data on websites on 12 of the biggest drugstores in the United States, including grocery store chains with pharmacies, and sharing the sensitive information with companies like Meta and Google, through their advertising and analytics products and Microsoft, through its search engine, Bing."[9]

14. Rather than attempt to collect more and more confidential and protected health information, telehealth and diagnostic test kit companies should minimize data collection and storage to what is necessary to provide health care services. In practice, few do; rather, likely

---

spectacularly-at-privacy-security/ (last visited Mar. 9, 2024).

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

[8] *See* Danielle Ellis, *Need to get Plan B or an HIV test online? Facebook may know about it*, KFF HEALTH NEWS & THE MARKUP (June 30, 2023), https://kffhealthnews.org/news/article/drugstores-pixel-sensitive-data-social-media-companies/ (last visited Mar. 9, 2024).

[9] *Id.*

cognizant that consumers would not voluntarily provide this sensitive and protected information, these companies resort to doing so covertly by installing invisible tracking technologies on their websites to collect and monetize that data.[10]

15. Moreover, many companies do not publicly disclose what types of data will be shared — for instance, whether it will include someone's contact information or aspects of their health data. By disclosing customer data to third parties for commercial use and providing little transparency into what data is shared and with whom, test providers make it more likely that sensitive data could be leaked, used to discriminate, and/or sold (and re-sold) by data brokers without oversight or consent.[11]

16. These companies—including Defendant—are facilitating their surreptitious connection and disclosure of protected health and other information by using tracking tools, popularly called "pixels," which collect information while a website runs.

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

---

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

[11] Kaylana Mueller-Hsia & Laura Hecht-Fellala, *Evaluating the Privacy of At-Home Covid 19 Tests, The Tests Are Essential for Fighting the Pandemic, but Poor Privacy Policy Practices Could Discourage Some People from Using Them*, BRENNAN CENTER FOR JUSTICE (Jan. 19, 2021), available at https://www.brennancenter.org/our-work/analysis-opinion/evaluating-privacy-covid-19-home-tests#:~:text=To%20maximize%20privacy%20protections%2C%20test,however%2C%20adhere%20to%20these%20principles (last visited Mar. 9, 2024).

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

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

20. Simply put, the Pixels secretly enable the unauthorized transmission and disclosure of Plaintiffs' and Class Members' highly sensitive Private Information by Defendant. To begin, these websites' pixels send several unique personal identifiers, including a User's Facebook ID and their internet protocol ("IP") address—which is protected information under the Health Insurance Portability and Accountability Act ("HIPAA")—to social media giants and other firms.[13]

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

[13] *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 (updated March 18, 2024 (last visited April 2, 2024).

21. They also send cookies – a way of storing information in a user's browser that helps track a user from page to page as the user browses a retailer's site.[14]

22. In addition to the IP address and cookies, the Pixels often send information about what items a consumer has viewed, clicked and purchased, including extremely sensitive and personal items, such as HIV tests and Plan B medications.

23. These pixels are often configured to share detailed "interaction data" with third-party advertising platforms. For instance, many of the retailers examined alerted at least one tech platform when shoppers clicked "add to cart" as they shopped for retail goods, a capacious category that included sensitive products like prenatal vitamins, pregnancy tests and Plan B emergency contraception.[15]

24. Unfortunately, Everlywell, a telehealth company that sells medical test kits for private at-home testing, is one such company. In order to provide these services, Everlywell owns, controls and maintains the website https://www.everlywell.com/ (referred to herein as the "Website"), which requires individuals to provide Private Information in order to create accounts and to participate in highly sensitive and personal health screenings and to view and to purchase diagnostic kits, among other things.

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

---

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

[15] *See*, *supra*, n.6.

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

27. This case concerns a very serious breach of Everlywell's data privacy and security obligations as it installed these tracking technologies on its Website to collect and to disclose to unauthorized third parties Plaintiffs' and Class Members' Private Information for the purpose of disclosing that information to Meta and other third parties, in violation of HIPAA and common law, solely for its own pecuniary gain.

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

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

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

31. Additionally, and upon information and good faith belief, Everlywell surreptitiously collects Plaintiffs' and Class Members' Private Information to use it for retargeting,

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

32. What Everlywell has not publicly acknowledged is that customers would be unknowingly sacrificing their privacy by using its Website. That is, Everlywell made the conscious and intentional decision to put its profits over the privacy of its Users, which number over one million.[16]

33. When Plaintiffs and other customers used Defendant's Website in order to search for and to obtain healthcare products, the names and types of their extremely sensitive healthcare products, including but not limited to, Hepatitis C test, sexually transmitted infections and diseases ("STI" and "STD") tests, diabetes management tests and numerous other products used to diagnose and/or treat highly sensitive and private medical conditions, were secretly disclosed to Facebook and other unauthorized third parties, along with their personal information and personal identifiers.

34. As detailed herein, Everlywell's privacy policies provided no warning whatsoever that Class Members' PHI and/or other sensitive health information would be disclosed to Facebook and other unauthorized third parties for marketing purposes or otherwise. Rather, the applicable privacy policies stated that written authorization must be obtained from customers before their PHI is used or disclosed for marketing purposes.[17]

35. Everlywell ***never*** obtained such authorizations from Plaintiffs or the Class Members. At all times relevant to this action, Plaintiffs and Class Members had no informed

---

[16] *See* https://www.everlywell.com/blog/news-and-info/results-your-body-can-count-on/ (last visited Mar. 9, 2024).

[17] *See* Defendant's *HIPAA Notice of Privacy practices*, https://www.everlyhealth.com/hipaa-notice/ (last accessed Mar. 9, 2024); *Consumer Protections*, https://www.everlywell.com/blog/news-and-info/where-to-buy-everlywell-tests/.

consent that information about their sensitive health conditions would be transmitted to the largest social media company on earth, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue.[18]

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

37. Thus, operating as implemented by Everlywell, the Pixels, Conversions API and other tracking technologies allow the Private Information that Plaintiffs and Class Members submit in confidence to be unlawfully disclosed to Facebook alongside the individual's name and other identifying information, including his or her Facebook ID, IP addresses and other identifying information pertaining to any accounts they may have with Facebook. This surreptitious and illegal collection and divulgence occurs on every webpage in which Everlywell installed the Pixels and for which it enabled Conversions API.

[18] This Court will not have to look far to find evidence of Meta's violations of privacy laws. Just in May of last year the European Union fined Meta "a record-breaking" $1.3 billion for violating EU privacy laws. *See* Hanna Ziady, *Meta slapped with record $1.3 billion EU fine over data privacy*, https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html (last accessed Mar. 9, 2024).

38. Despite warnings that healthcare companies were disclosing Private Information to social media companies by embedding and using Pixels and/or similar tracking technologies as far back as at least February 2020, Everlywell breached confidentiality and violated Plaintiffs' and Class Members' privacy when it chose to embed the Pixels and other tracking codes to share Private Information with third parties.[19]

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

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

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… ***If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.*** [20]

---

[19] Molly Osberg & Dhruv Mehrotral, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137 (last visited Mar. 9, 2024); *see also* Timothy M. Hale, PhD & Joseph C. Kvedar, MD, *Privacy and Security Concerns in Telehealth* (Dec. 2014), https://journalofethics.ama-assn.org/article/privacy-and-security-concerns-telehealth/2014-12, AMA JOURNAL OF ETHICS (illustrating that problems with privacy and telehealth apps started to surface as early as 2014) (last visited Mar. 9, 2024).

[20] *Guidance regarding Methods for De-identification of Protected Health Information in*

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

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[21]

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

---

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 Mar. 9, 2024) (noting that "HIPAA Identifiers" include name; address (all geographic subdivisions smaller than state, including street address, city county, and zip code); all elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age); telephone numbers; email address; medical record number; health plan beneficiary number; account number; device identifiers and serial numbers; web URL; internet protocol (IP) address; and any other characteristic that could uniquely identify the individual).

[21] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (emphasis added) (updated March 18, 2024 (last visited April 2, 2024).

and (vi) otherwise failing to design and monitor its Website to maintain the security, confidentiality and integrity of patient Private Information.

43. Despite incorporating the Pixels and Conversions API into its Website and servers, Everlywell has never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook.[22]

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

45. Plaintiffs therefore seek on behalf of themselves and a class of similarly situated persons, to remedy these harms and therefore assert the following statutory and common law claims against Everlywell: (i) Negligence; (ii) Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2511(1), *et seq*., Unauthorized Interception, Use and Disclosure; (iii) Violation of Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. 505/1 *et seq.*; (iv) Violation of Illinois Eavesdropping Statute, 720 Ill. Comp. Stat. 5/14 *et seq*.; (v) Nevada

[22] In contrast to Defendant, in recent months several medical providers which have installed the Facebook Pixel on their web properties have provided their patients with notices of data breaches caused by the Pixels transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf; *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies* (Oct. 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3; *Novant Health Notifies 1.3M Patients of Unauthorized PHI Disclosure Caused By Meta Pixel* (Aug. 17, 2022), https://healthitsecurity.com/news/novant-health-notifies-patients-of-unauthorized-phi-disclosure-caused-by-meta-pixel (last visited April 3, 2024).

Deceptive Trade Practices Act, NRS ch. 598; and (vi) Maryland Wiretap Act, Md. Code Ann., Cts. & Jud. Proc. § 10-402, *et seq*.

PARTIES

A. Plaintiff Joshua Cook

46. Plaintiff Joshua Cook is a citizen of the state of Illinois residing in Winnebago County and brings this action in an individual capacity and on behalf of all others similarly situated.

47. In February and March 2021 as well as March and July 2022, Plaintiff Cook utilized Defendant's Website at least six times on his personal electronic devices to research and purchase medical at-home test kits such as [redacted].

48. While seeking those services and treatments, Everlywell required Plaintiff to provide—and Plaintiff provided—personal health information including his name, email address, phone number, address and medical conditions.

49. While Plaintiff Cook was a user of Everlywell services, he never consented to or authorized the use of his Private Information by third parties or to Defendant enabling third parties to access, interpret and use such Private Information.

50. Plaintiff Cook had an active Facebook account while he used Defendant's services, and he accessed Defendant's Website while logged into his Facebook account on the same device.

51. After providing his Private Information to Defendant through the Website, Plaintiff Cook immediately began seeing targeted health ads [redacted] on his Facebook account.

52. Upon information and good faith belief, Plaintiff began receiving these ads after his PII and PHI was disclosed by Defendant's Pixel to Facebook, which accessed and analyzed that information to identify Plaintiff's Facebook account and determine which advertisements

would most effectively target his medical condition, in this case his [redacted] status. Facebook in turn shared the information with other unauthorized third parties so that they could determine if their ads would effectively target that condition.

53. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, Defendant intercepted at least the following communications about Plaintiff's medical condition, diagnosis, and treatment, via the following long-URLs or substantially similar URLs that were sent to Meta via the Pixel (and which contain information concerning Plaintiff's specific medical conditions, queries, as well as treatments sought):

[redacted]

B. Plaintiff Melody Schoon

54. Plaintiff Melody Schoon is a citizen of the state of Illinois residing in Boone County and brings this action in an individual capacity and on behalf of all others similarly situated.

55. In April and October 2021, Plaintiff Schoon utilized Defendant's Website at least six times on her personal electronic devices to research and purchase sensitive medical tests including but not limited to, a [redacted]

56. While seeking those services and treatments, Everlywell required Plaintiff to provide—and Plaintiff provided—personal health information including her name, email address, phone number, address and medical conditions.

57. While Plaintiff Schoon was a user of Everlywell 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.

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

59. After providing her Private Information to Defendant through the Website, Plaintiff Schoon immediately began seeing targeted health ads related to her health condition on her Facebook account.

60. Upon information and good faith belief, Plaintiff began receiving these ads after her PII and PHI was disclosed by Defendant's Pixel to Facebook, which accessed and analyzed that information to identify Plaintiff's Facebook account and determine which advertisements would most effectively target her medical condition. Facebook in turn shared the information with other unauthorized third parties so that they could determine if their ads would effectively target that condition.

61. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, Defendant intercepted at least the following communications about Plaintiff's medical condition, diagnosis, and treatment,, via the following long-URLs or substantially similar URLs that were sent to Meta via the Pixel (and which contain information concerning Plaintiff's specific medical conditions, queries and treatments sought):

[redacted]

[redacted]

C. Plaintiff Jasmine Smith

62. Plaintiff Jasmine Smith is a citizen of the state of Illinois residing in Cook County and brings this action in an individual capacity and on behalf of all others similarly situated.

63. In 2022, Plaintiff Smith utilized Defendant's Website on her personal electronic devices to research and purchase sensitive medical tests including but not limited to, a [redacted]

64. While seeking those services and treatments, Everlywell required Plaintiff to provide—and Plaintiff provided—personal health information including her name, email address, phone number, address and medical conditions.

65. While Plaintiff Smith was a user of Everlywell 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.

66. Plaintiff Smith 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.

67. After providing her Private Information to Defendant through the Website, Plaintiff Smith immediately began seeing targeted health ads [redacted] on her Facebook account.

68. Upon information and good faith belief, Plaintiff began receiving these ads after her PII and PHI was disclosed by Defendant's Pixel to Facebook, which accessed and analyzed that information to identify Plaintiff's Facebook account and determine which advertisements would most effectively target her medical condition. Facebook in turn shared the information with other unauthorized third parties so that they could determine if their ads would effectively target that condition.

69. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, Defendant

intercepted at least the following communications about Plaintiff's medical condition, diagnosis, and treatment,, via the following long-URLs or substantially similar URLs that were sent to Meta via the Pixel (and which contain information concerning Plaintiff's specific medical conditions, queries and treatments sought):

[redacted]

D. Plaintiff Ashley Reedy

70. Plaintiff Ashley Reedy is a citizen of the state of Maryland residing in Baltimore County and brings this action in an individual capacity and on behalf of all others similarly situated.

71. In December 2021, Plaintiff Reedy utilized Defendant's Website on her personal electronic devices to research and purchase sensitive medical tests including [redacted].

72. While seeking those services and treatments, Everlywell required Plaintiff to provide—and Plaintiff provided—personal health information including her name, email address, phone number, address and medical conditions.

73. While Plaintiff Reedy was a user of Everlywell 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.

74. Plaintiff Reedy 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.

75. After providing her Private Information to Defendant through the Website, Plaintiff Reedy immediately began seeing targeted health ads [redacted] on her Facebook account.

76. Upon information and good faith belief, Plaintiff began receiving these ads after her PII and PHI was disclosed by Defendant's Pixel to Facebook, which accessed and analyzed that information to identify Plaintiff's Facebook account and determine which advertisements would most effectively target her medical condition. Facebook in turn shared the information with other unauthorized third parties so that they could determine if their ads would effectively target that condition.

77. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, Defendant intercepted at least the following communications about Plaintiff's medical condition, diagnosis, and treatment, via the following long-URLs or substantially similar URLs that were sent to Meta via the Pixel (and which contain information concerning Plaintiff's specific medical conditions, queries and treatments sought):

[redacted]

E. Plaintiff Shadari Bush

78. Plaintiff Shadari Bush is a citizen of the state of Nevada residing in Clark County and brings this action in an individual capacity and on behalf of all others similarly situated.

79. In March 2021, Plaintiff Bush utilized Defendant's Website on her personal electronic devices to research and purchase sensitive medical tests including [redacted].

80. While seeking those services and treatments, Everlywell required Plaintiff to provide—and Plaintiff provided—personal health information including her name, email address, phone number, address and medical conditions.

81. While Plaintiff Bush was a user of Everlywell 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.

82. Plaintiff Bush 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.

83. After providing her Private Information to Defendant through the Website, Plaintiff Bush immediately began seeing targeted health ads for [redacted], on her Facebook account.

84. Upon information and good faith belief, Plaintiff began receiving these ads after her PII and PHI was disclosed by Defendant's Pixel to Facebook, which accessed and analyzed that information to identify Plaintiff's Facebook account and determine which advertisements would most effectively target her medical condition. Facebook in turn shared the information with other unauthorized third parties so that they could determine if their ads would effectively target that condition.

85. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, Defendant intercepted at least the following communications about Plaintiff's medical condition, diagnosis, and treatment,, via the following long-URLs or substantially similar URLs that were sent to Meta via the Pixel (and which contain information concerning Plaintiff's specific medical conditions, queries and treatments sought):

[redacted]

F. Defendant Everlywell

86. Defendant Everlywell is a foreign corporation incorporated in Delaware and headquartered at 823 Congress Ave, Suite 1200, in Austin, Texas.

JURISDICTION & VENUE

87. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative Class Members and minimal diversity exists because Plaintiffs and many putative Class Members are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

88. This Court has personal jurisdiction over Everlywell because Defendant has intentionally directed its business activities in Illinois, targeting the Illinois market, and purposefully availed itself of the privilege of conducting business in this state, including by providing board-certified physicians licensed in Illinois to patients for consults[23] and by making prescriptions available for customers in the state of Illinois.[24] In addition, the conduct underlying the claims that caused Plaintiffs' injuries took place in Illinois, that is, Defendant's interception and disclosure of Plaintiffs' Private Information occurred in this state which was foreseeable to Defendant..

89. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because: a substantial part of the events giving rise to this action occurred in this District, including Everlywell's interception and unlawful disclosure of Class Members' Private Information and Everlywell caused harm to Class Members residing in this District.

---

[23] *See What Diagnostic Tests Does Everlywell Offer?*, https://support.everlywell.com/article/365-what-diagnostic-tests-does-everlywell-offer (last accessed April 3, 2024).

See Prescription Availability By State, https://support.everlywell.com/article/127-std-prescription-availability-by-state (last accessed April 3, 2024).

FACTUAL ALLEGATIONS

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

90. A "pixel" is a piece of code that "tracks the people and the types of actions they take"[25] as they interact with a website, including how long a person spends on a particular webpage, which buttons the person clicks, which pages they view, the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box) and much, much more.

91. When embedded on a company's website, the Pixels send data about user activity, including what you are viewing, your searches on websites, purchases you have made, items added to a shopping cart, and even information you filled out in online forms.[26] Meta calls this activity "interactions."

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

93. 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.

---

[25] *Retargeting*, https://www.facebook.com/business/goals/retargeting (last visited Mar. 9, 2024).

[26] *See* Tom Kemp, *"Oops! I Did It Again" … Meta Pixel Still Hoovering Up Our Sensitive Data* (July 2, 2023), https://tomkemp00.medium.com/oops-i-did-it-again-meta-pixel-still-hoovering-up-our-sensitive-data-f99c7b779d47 (last visited Mar. 9, 2024).

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

95. The Pixels can also share the user's identifying information for easy tracking via the "cookies"[27] stored on their computer by any of the Pixel Information Recipients with which they have an account.

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

97. 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.

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

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

[27] "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 Mar. 9, 2024).

99. Throughout the Class Period, Defendant maintained and operated websites (including www.everlywell.com), by and through which Defendant encouraged and permitted consumers to seek healthcare products.

100. To purchase sensitive healthcare products used to treat and diagnose their medical conditions, Plaintiffs and other Class Members were required to search for and to add the healthcare products to their virtual cart before proceeding to checkout.

101. On information and good faith belief, each step of this process was tracked and logged by the Meta Pixel.

102. On information and good faith belief, throughout the Class Period, the process for purchasing healthcare products on the Website has been substantially the same in all material respects throughout the United States.

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

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

104. Completely unbeknownst to Plaintiff and other Class Members, and continuing to the present, Private Information that they communicated to Defendant through the Website while purchasing sensitive healthcare products was intercepted by and/or disclosed to at least four unauthorized third parties: Meta, Google, Bing and Twitter.[28]

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

[28] *See, supra,* n.8.

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

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

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

> - **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
>
> - **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.
>
> - **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data. [29]

108. A customer's HTTP Request essentially asks the Website to retrieve certain information (such as sensitive healthcare products placed in the virtual shopping cart), and the

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

HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the customer's screen as they navigate the Website).

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

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

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

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

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

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

115. Defendant intentionally configured Pixels installed on its Website to capture both the "characteristics" of individual patients' communications with the Defendant's Websites (e.g., their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (i.e., the buttons, links, pages, and tabs they click and view, as well as search terms entered into free text boxes and descriptive URLs showing the information being exchanged).

116. 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. 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.

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

118. 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.

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

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

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

122. The Meta Pixel, a marketing product, is a "piece of code" that allowed Defendant to "understand the effectiveness of [their] advertising and the actions [customers] take on [their] site."[30] It also allowed Defendant to optimize the delivery of ads, measure cross-device conversions, create custom advertising groups or "audiences," learn about the use of its Website, and decrease advertising and marketing costs.[31]

123. Most importantly, it allowed Facebook to secretly intercept customers' communications about their purchases of sensitive healthcare products including LIST and

---

[30] https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Mar. 9, 2024).

[31] *Id.*

numerous other products to diagnose and/or treat highly sensitive and private conditions on the Website.

B. Facebook's Platform & its Business Tools.

124. 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.[32]

125. 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.

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

127. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL"), metadata, button clicks, and other user interactions with a webpage.[33]

---

[32] META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx, INVESTOR.FB.COM (last visited Mar. 9, 2024).

[33] *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Mar. 9, 2024); *see* META PIXEL, GUIDES, ADVANCED, https://developers.facebook.com/docs/meta-pixel/advanced (last visited Mar. 9, 2024); *see also* BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142 (last visited Mar. 9, 2024); META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Mar. 9, 2024).

128. Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[34]

129. One such Business Tool is the tracking Meta Pixel which "tracks the people and type of actions they take."[35]

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

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

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

---

[34] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Mar. 9, 2024).

[35] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Mar. 9, 2024).

133. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[36] Plaintiffs' and Class Members' identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

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

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

136. This disclosed PHI and PII allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought (in the case of Defendant, purchasing sensitive healthcare products including LIST and numerous other products to diagnose and/or treat highly sensitive and private conditions), and Facebook then sells that information to marketers who will online target Plaintiffs and Class Members.

---

[36] *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 Mar. 9, 2024).

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

137. The disclosure of Plaintiffs' and Class Members' Private Information via the Pixels contravenes the letter and spirit of HIPAA's "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") which governs how health care providers must safeguard and protect Private Information.[37]

138. The HIPAA Privacy Rule sets forth policies to protect all Individually Identifiable Health Information ("IIHI") that is held or transmitted by a covered entity such as Defendant. These are the 18 HIPAA Identifiers that are considered personally identifiable information because this information can be used to identify, contact, or locate a specific person or can be used with other sources (such as a person's Facebook account) to identify a single individual. When IIHI is used in conjunction with one's physical or mental health or condition, health care, and/or one's payment for that health care, it becomes PHI.[38]

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

---

[37] *The HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited Mar. 9, 2024).

[38] *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (HIPAA Identifiers include name; address (all geographic subdivisions smaller than state, including street address, city county, and zip code); all elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age); telephone numbers; email address; medical record number; health plan beneficiary number; account number; device identifiers and serial numbers; web URL; internet protocol (IP) address; and any other characteristic that could uniquely identify the individual) (last visited Mar. 9, 2024).

140. 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]

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

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

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

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

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

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

144. In addition, the Office for Civil Rights at HHS' Bulletin expressly provides that "**[r]egulated entities are not permitted to use tracking technologies in a manner that would**

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

result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."[40]

145. Tracking technology vendors like Facebook and Google are considered business associates under HIPAA where, as here, they provide services to Defendant and receive and maintain PHI.

> Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (*e.g.* health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.[41]

146. The Bulletin further explained that health care providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address) even if no treatment information is included and even if the individual does not have a relationship with the health care provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> **Some regulated entities may be disclosing a variety of information to tracking technology vendors through tracking**

[40] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (emphasis added) (updated March 18, 2024 (last visited April 2, 2024)).

[41] *Id.*

> **technologies placed on the regulated entity's website or mobile app, such as information that the individual types or selects when they use regulated entities' websites or mobile apps**. The information disclosed 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, device IDs, or any unique identifying code.
>
> ---
>
> IIHI collected on a regulated entity's website or mobile app generally is PHI, **even if the individual does not have an existing relationship with the regulated entity** and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.[42]

147. HIPAA applies to Defendant's webpages with tracking technologies even outside the patient portal:

> Tracking on unauthenticated webpages
>
> Regulated entities may also have unauthenticated webpages, which are webpages that do not require users to log in before they are able to access the webpage, such as a webpage with general information about the regulated entity like their location, visiting hours, employment opportunities, or their policies and procedures… **in some cases, tracking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to the tracking technology vendors**. Regulated entities are required to "[e]nsure the confidentiality, integrity, and availability of all electronic PHI the [regulated entity] creates, receives, maintains, or transmits." Thus, regulated entities that are considering the use of online tracking technologies should consider whether any PHI will be transmitted to a tracking technology vendor, and take appropriate steps consistent with the HIPAA Rules.[43]

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

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

148. HHS explained that, if the online tracking technologies on the webpages have access to information that relates to an individual's past, present, or future health, health care, or payment for health care, that is a disclosure of PHI, for example:

> [I]f an individual were looking at a hospital's webpage **listing its oncology services** to seek a second opinion on treatment options for their brain tumor, **the collection and transmission of the individual's IP address, geographic location, or other identifying information showing their visit to that webpage is a disclosure of PHI** to the extent that the information is both identifiable and related to the individual's health or future health care.

149. HHS also explained in the Bulletin that tracking technologies on health care providers' patient portals "generally have access to PHI" and may access diagnoses and treatment information, in addition to other sensitive data:

> Tracking on user-authenticated webpages
>
> Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. **Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to only use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.[44]

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

150. The Bulletin is not a pronouncement of new law, but instead a reminder to covered entities and business associates of their longstanding obligations under existing guidance.

151. The Bulletin notes that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," then explains how online tracking technologies violate the same HIPAA rules that have existed for decades.[45]

152. In other words, HHS has expressly stated that Defendant has violated HIPAA Rules by implementing the Meta Pixel.

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

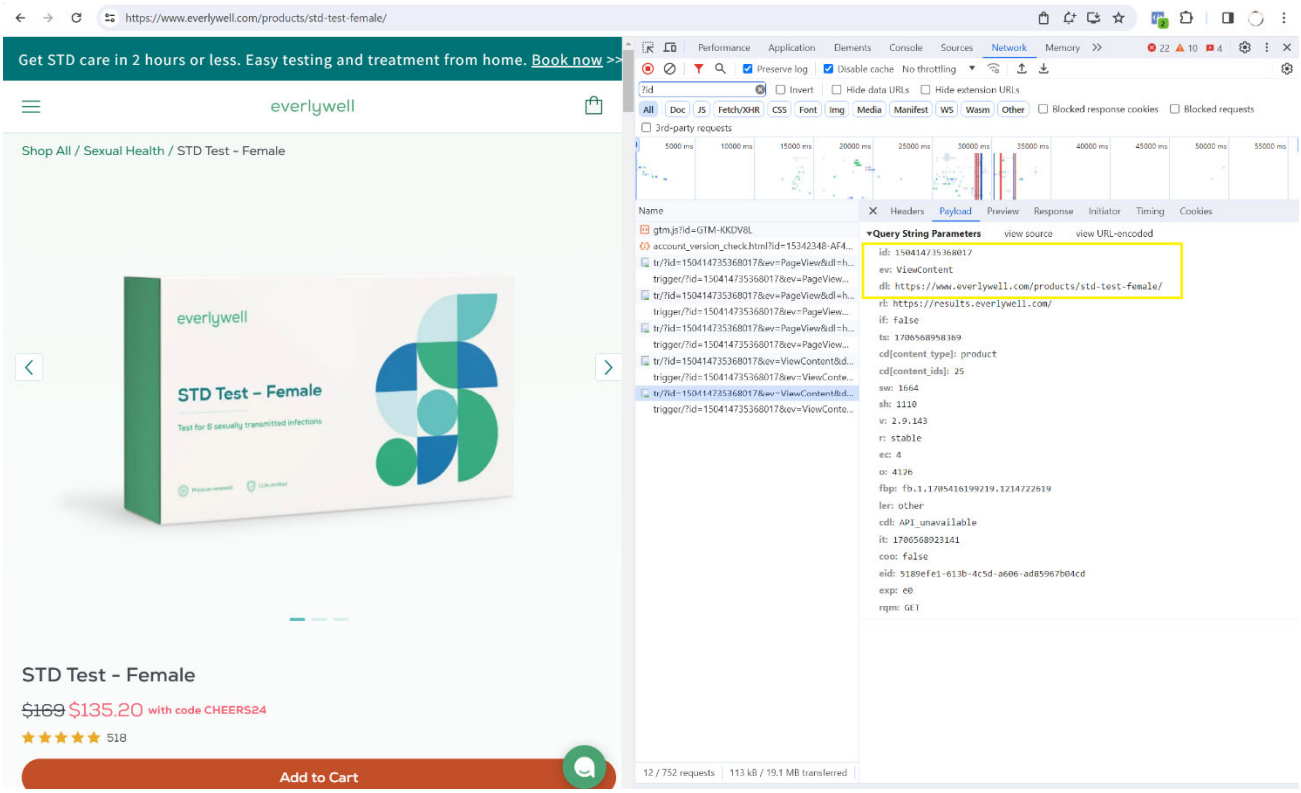
153. Starting on a date unknown and continuing to the present, Defendant embedded the Meta Pixel on and throughout its Website and transmitted Private Information shared by Plaintiffs and Class Members, without their consent, to Meta in accordance with the Meta Pixel's configuration.

154. Defendant installed the Meta Pixel on its website - www.everlywell.com. When Plaintiffs or another Class Member visited that website and completed the steps necessary to purchase sensitive healthcare products including Hepatitis C, STD and STI, pregnancy, diabetes management and numerous other products to diagnose and/or treat highly sensitive and private

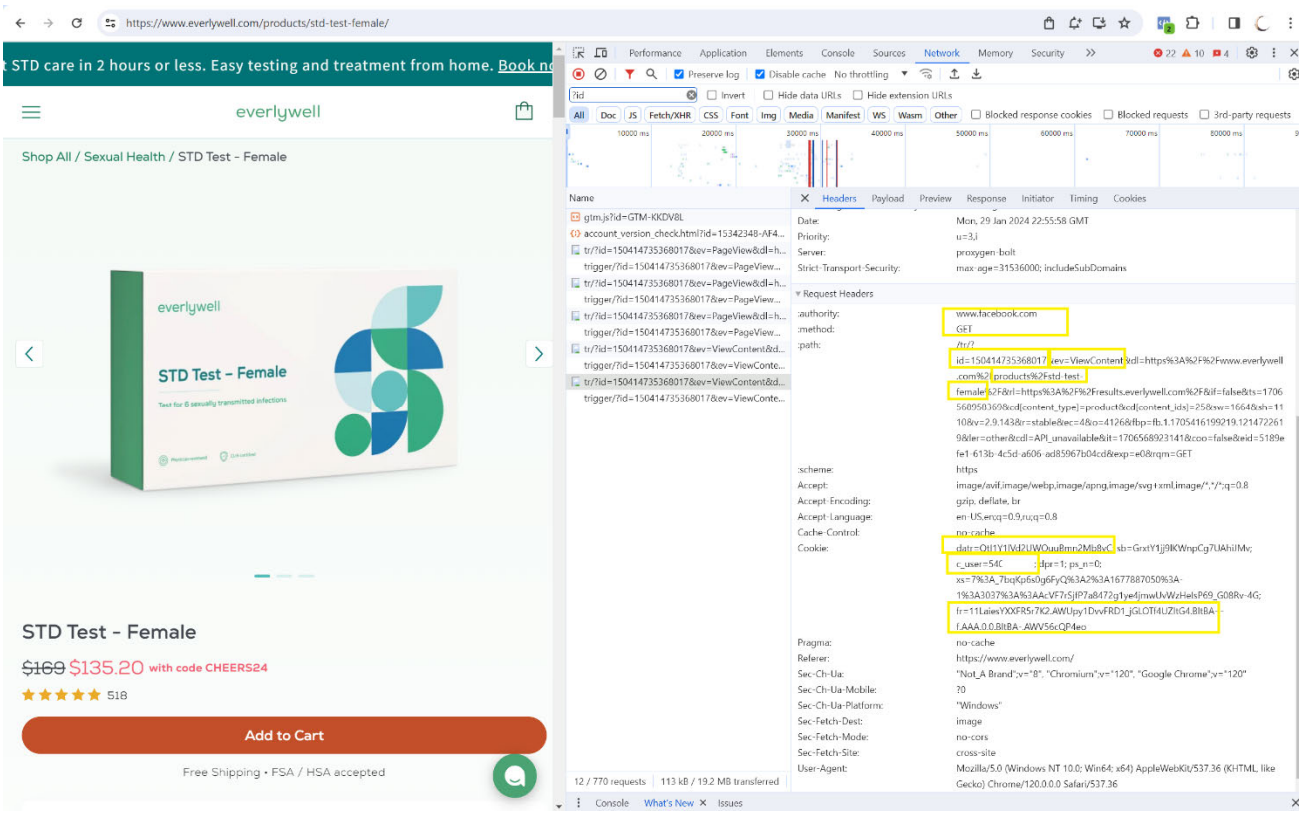
[45] *Id.* (citing, *e.g.*, Modifications of the HIPAA [Rules], Final Rule," 78 FR 5566, 5598, a rulemaking notice from January 25, 2013, which stated: "[P]rotected health information … may not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a covered entity, then it is protected health information by definition since it is indicative that the individual received health care services or benefits from the covered entity, and therefore it must be protected … in accordance with the HIPAA rules." at fn. 22).

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

Figures 1 & 2: Examples of a HTTP single communication session sent from the customer's device to Facebook that reveals the fact that the customer is searching for an STD test for females and the customer's unique personal identifiers including the FID (c_user field)[46]:



[46] The user's Facebook ID is represented as the c_user ID highlighted in the image above, and Plaintiffs have redacted the corresponding string of numbers to preserve the user's anonymity.

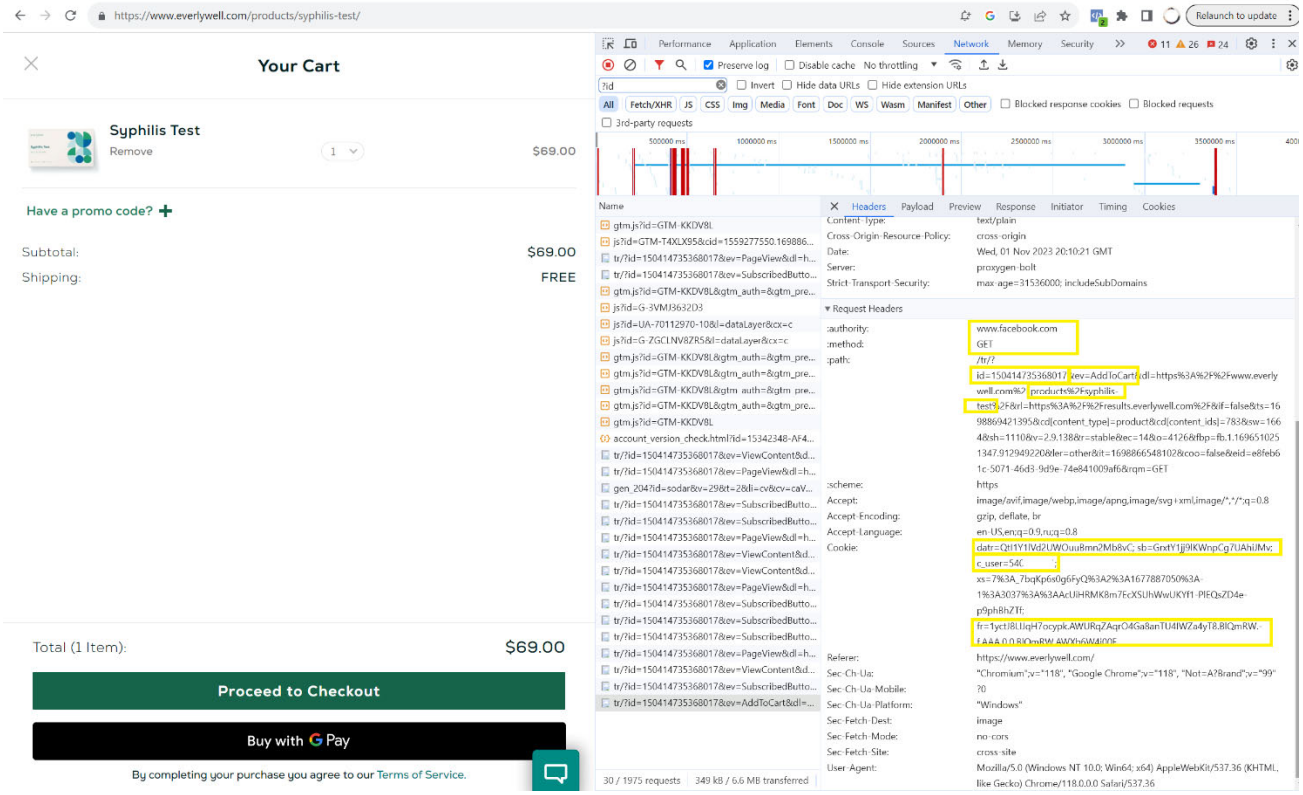


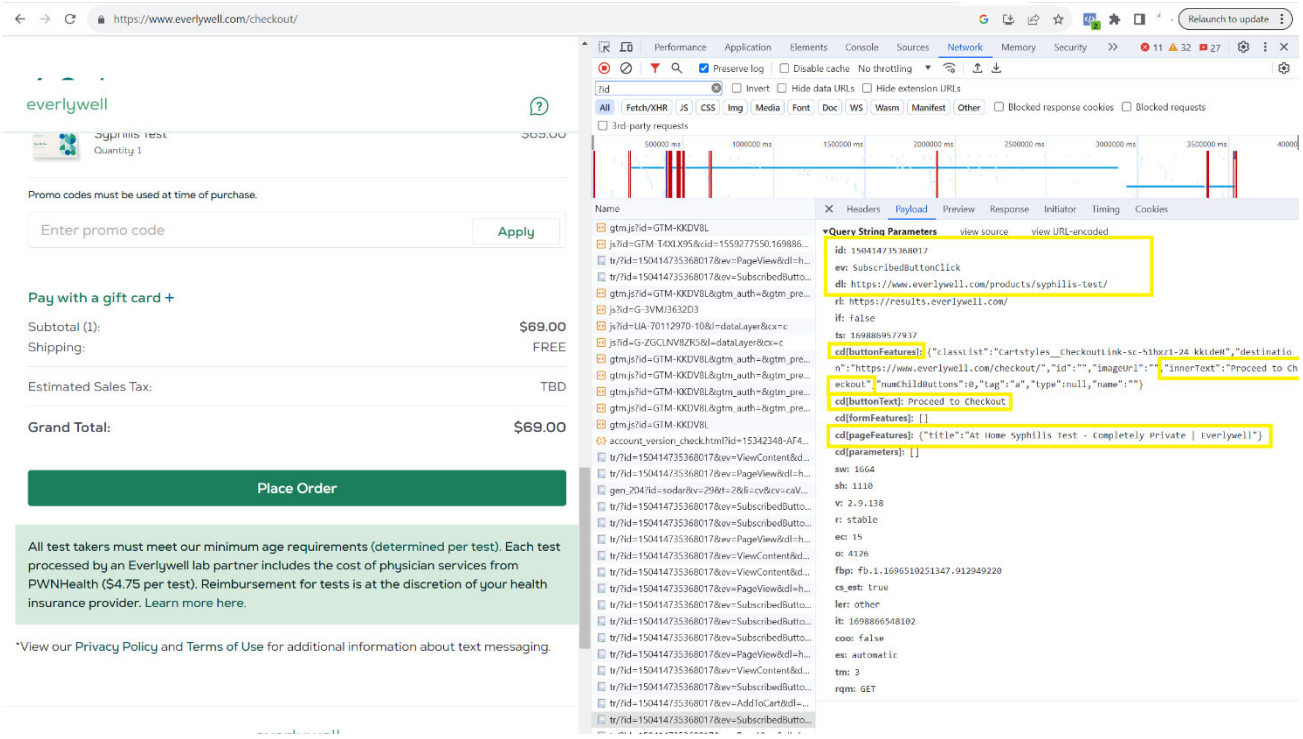
155. In the examples above, the "id" value is the unique number of the Meta Pixel Defendant chose to embed in its Website, and the "ev" is the type of website interaction "event" that is being captured by the Pixel.

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

Figures 3 & 4: Examples of HTTP communication sessions sent from the customer's device to Facebook that reveal the fact that the customer is purchasing a test for syphilis, via

"AddToCart" and "SubscribedButtonClick" events, along with the customer's unique personal identifiers including the FID (c_user field) and the exact text of buttons clicked like "Proceed to Checkout":



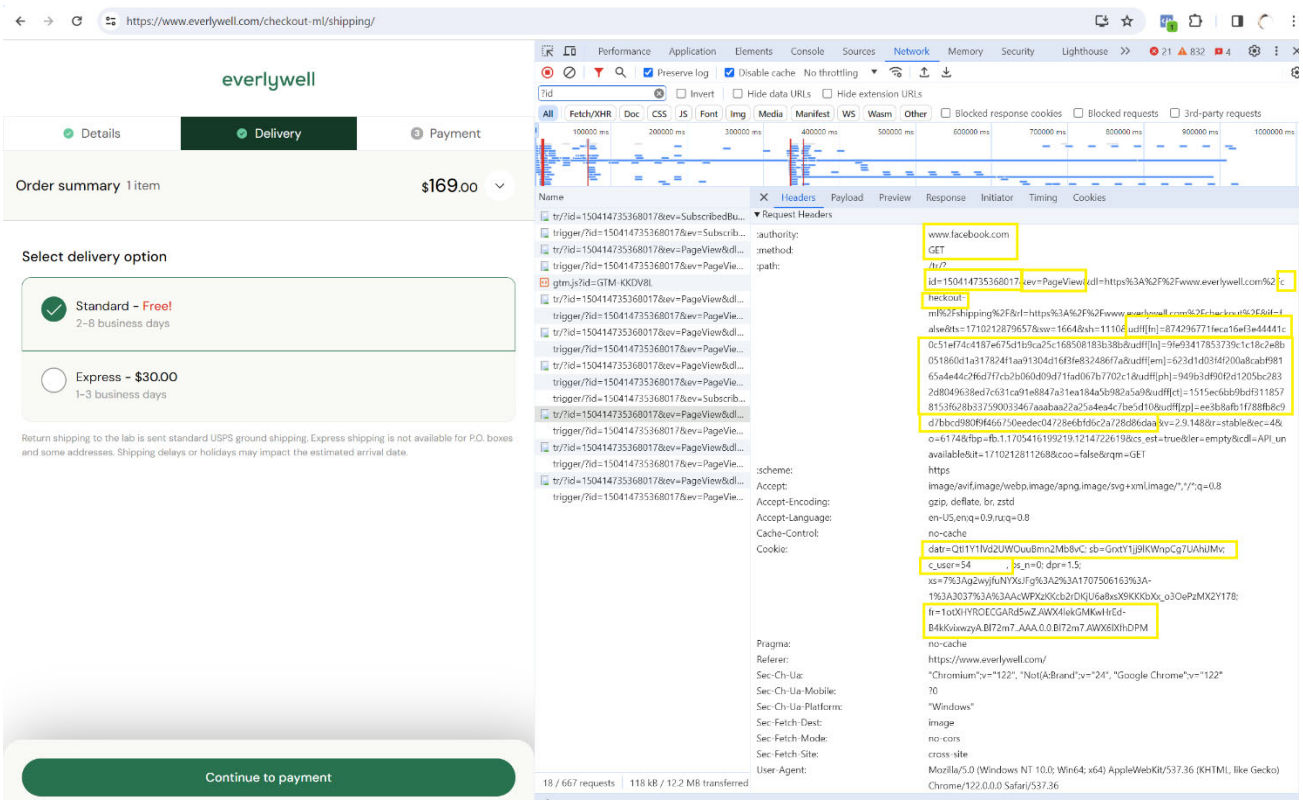


157. Moreover, the Meta Pixel on Defendant's website was also intentionally configured or authorized to use a feature called "automatic advanced matching." That feature scans forms on a website looking for fields that may contain personally identifiable information like a first name, last name, email address, or phone number and then causes that information to be disclosed to Meta. On Defendant's website this feature collected, at a minimum, the first names and last names of Plaintiffs and other Class Members as displayed on the checkout page of the Website, their email addresses, phone numbers, and zip codes.

Figures 5 & 6: Example of HTTP communication session sent from the customer's device to Facebook that reveals the customer's name (udff[fn] and udff[ln] values), email (udff[em] value), phone number (udff[ph] value) and zip code (udff[zp] value):

▼**Query String Parameters** view source view URL-encoded

id: 150414735368017
ev: PageView
dl: https://www.everlywell.com/checkout-ml/shipping/
rl: https://www.everlywell.com/checkout/
if: false
ts: 1710212879657
sw: 1664
sh: 1110
udff[fn]: 874296771feca16ef3e44441c0c51ef74c4187e675d1b9ca25c168508183b38b
udff[ln]: 9fe93417853739c1c18c2e8b051860d1a317824f1aa91304d16f3fe832486f7a
udff[em]: 623d1d03f4f200a8cabf98165a4e44c2f6d7f7cb2b060d09d71fad067b7702c1
udff[ph]: 949b3df90f2d1205bc2832d8049638ed7c631ca91e8847a31ea184a5b982a5a9
udff[ct]: 1515ec6bb9bdf3118578153f628b337590033467aaabaa22a25a4ea4c7be5d10
udff[zp]: ee3b8afb1f788fb8c9d7bbcd980f9f466750eedec04728e6bfd6c2a728d86daa
v: 2.9.148
r: stable
ec: 4
o: 6174
fbp: fb.1.1705416199219.1214722619
cs_est: true
ler: empty
cdl: API_unavailable
it: 1710212811268
coo: false
rqm: GET



158. The data collected by the automatic advanced matching feature is disclosed to Meta in an obfuscated form known as a "hash." But Meta is able to determine the pre-obfuscated version of the data. Indeed, Meta uses the hashed information to link other data collected and disclosed by the Meta Pixel to Plaintiffs' and Class Members' Facebook and Instagram profiles.

159. Thus, put simply, when Plaintiffs or other Class Members used Defendant's website to purchase sensitive healthcare products including Hepatitis C, STD and STI, pregnancy, diabetes management and numerous other products to diagnose and/or treat highly sensitive and private conditions, their identities, personal identifiers, and health information (including their medical conditions and treatments sought) were disclosed to Meta.

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

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

161. Defendant's privacy policies, including its current policies and historical policies during the Class Period, represent to Plaintiffs and Class Members that it will keep their Private Information private and secure, and that it will only disclose Private Information under certain circumstances – ***none of which is true***.

162. These Privacy Policies state that Plaintiffs' and Class Members' PHI will not be shared for marketing purposes without prior, written permission.

163. Plaintiffs and Class Members have not provided Defendant with written permission to share their PHI for marketing purposes.

164. Moreover, Defendant's privacy policies, despite their increasing breadth over the years with respect to sharing customers' data, have never specifically disclosed to Plaintiffs or Class Members that their viewing or purchase of sensitive healthcare products will be sent to social media companies for any purposes; nor has Defendant ever obtained informed consent from Plaintiff or Class Members to do so.

165. Defendant breached Plaintiffs' and Class Members' right to privacy by unlawfully disclosing their Private Information to the Pixel Information Recipients. Specifically, Plaintiffs and Class Members had a reasonable expectation of privacy (based on Defendant's own representations to Plaintiffs and the Class that Defendant would not disclose their Private Information to third parties).

166. Specifically, Defendant did not inform Plaintiffs that it was sharing 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.

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

168. Even non-Facebook users can be individually identified via the information gathered on the Website, like an IP address or personal device identifying information. This is precisely the type of information for which HIPAA requires the use of de-identification techniques to protect patient privacy.[47]

169. In fact, in an action pending against Facebook related to use of its Meta Pixel on a healthcare provider's website, Facebook explicitly stated it requires Pixel users to "post a prominent notice on every page where the pixel is embedded and to link from that notice to information about exactly how the pixel works and what is being collected through it, so it is not invisible."[48]

170. Defendant not only did not post such a notice, but it also falsely represented it would notify affected victims should a breach of unsecured PHI take place.

171. Facebook further stated that "most providers [...] will not be sending [patient information] to Meta because it violates Meta's contracts for them to be doing that."[49]

---

[47] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited Mar. 9, 2024).

[48] *See* Transcript of the argument on Plaintiff's Motion for Preliminary Injunction in *In re Meta Pixel Healthcare Litigation*, Case No. CV-22-03580-WHO (N.D. Cal. Nov. 9, 2022) (Hon. J. Orrick), at 19:12-18; *see also In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218 (N.D. Cal. Dec 22, 2022).

[49] *Id.*, *supra,* n.16, at 7:20-8:11.

172. Despite a lack of disclosure, Defendant allowed third parties such as Meta and/or Google to "listen in" on customers' confidential communications with Defendant and to intercept and use for advertising purposes the very information it promised to keep private. It did this in order to bolster its profits.

VII. USERS' REASONABLE EXPECTATION OF PRIVACY.

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

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

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

176. 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.[50]

177. Personal data privacy and obtaining consent to share Private Information were material to Plaintiffs and Class Members in their purchases of Defendant's medical products,

[50] *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 Mar. 9, 2024).

including their purchases of [redacted]

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

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

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

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

181. Based on information and belief, Defendant was advertising its services on Facebook, for one, and the Pixels were used to "help [Everlywell] understand which types of ads and platforms are getting the most engagement[.]"[51]

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

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

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

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

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

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

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

187. 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.[52]

188. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[53]

---

[52] *See* https://time.com/4588104/medical-data-industry/ (last visited Mar. 9, 2024).

[53] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Mar. 9, 2024).

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

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

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

192. Policymakers are proactively calling for a revision and potential upgrade of the HIPAA privacy rules out of concern for what might happen as tech companies continue to march into the medical sector.[54]

193. The Private Information at issue here is also a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use Private Information to commit an array of crimes that include identity theft and medical and financial fraud.[55] A robust "cyber black market" exists where criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

---

[54] *Id.*

[55] FTC, *Warning Signs of Identity Theft,* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Mar. 9, 2024).

194. While credit card information and associated IIHI can sell for as little as $1–$2 on the black market, PHI can sell for as much as $363.[56]

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

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

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

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

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

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

---

[56] Center for Internet Security, *Data Breaches: In the Healthcare Sector,* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed Mar. 9, 2024).

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

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

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

202. The tracking tools incorporated into, embedded in, or otherwise permitted on Defendant's Website were invisible to Plaintiffs and Class Members while using that Website. The Meta Pixels on Defendant's Website were seamlessly integrated into the Website such that there was no reason for Plaintiffs or any Class Member to be aware of or to discover their presence.

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

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

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

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

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

TOLLING, CONCEALMENT & ESTOPPEL

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

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

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

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

212. Defendant had exclusive knowledge that its Website incorporated the Meta Pixel and other tracking tools and yet failed to disclose to customers, including Plaintiffs and Class Members, that by purchasing sensitive healthcare products including Hepatitis C, STD and STI, pregnancy, diabetes management and numerous other products to diagnose and/or treat highly sensitive and private conditions through Defendant's Website, Plaintiffs' and Class Members' Private Information would be disclosed or released to Meta and other unauthorized third parties.

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

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

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

CLASS ALLEGATIONS

216. 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).

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

The Nationwide Class

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

218. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiffs Joshua Cook, Jasmine Smith and Melody Schoon assert claims on behalf of the Illinois Subclass, which is defined as follows:

The Illinois Subclass

> All natural persons residing in Illinois who used Defendant's Website to purchase human healthcare products to treat sensitive health conditions including reproductive and sexual health and diabetes management and whose Private Information was disclosed or transmitted to Meta or any other unauthorized third party.

219. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff Shandari Bush asserts claims on behalf of the Nevada Subclass, which is defined as follows:

The Nevada Subclass

> All natural persons residing in Nevada who used Defendant's Website to purchase human healthcare products to treat sensitive health conditions including reproductive and sexual health and diabetes management and whose Private Information was disclosed or transmitted to Meta or any other unauthorized third party.

220. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff Ashley Reedy asserts claims on behalf of the Maryland Subclass, which is defined as follows:

The Maryland Subclass

> All natural persons residing in Maryland who used Defendant's Website to purchase human healthcare products to treat sensitive health conditions including reproductive and sexual health and diabetes management and whose Private Information was disclosed or transmitted to Meta or any other unauthorized third party.

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

222. 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.

223. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. There are at least 1 million customers that have been impacted by Defendant's actions. Moreover, the exact number of those impacted is generally ascertainable by appropriate discovery and is in the exclusive control of Defendant.

224. **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 customers' Private Information;

g) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to keep the Private Information belonging to Plaintiffs and Class Members free from unauthorized disclosure;

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

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

j) Whether Defendant knowingly made false representations as to their 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.

225. **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.

226. **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.

227. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members in that all the Plaintiffs' and Class Members' data was unlawfully stored and disclosed to unauthorized third parties, including the Pixel Information Recipients, in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

228. **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.

229. 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.

230. 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.

231. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the unauthorized disclosures that have

taken place. Class Members have already been preliminarily identified and sent Notice by Defendant.

COUNT I

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

232. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

233. The ECPA protects both sending and receipt of communications.

234. 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.

235. The transmissions of Plaintiffs' PII and PHI to Defendant's Website qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

236. Electronic Communications. The transmission of PII and PHI between Plaintiffs and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

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

238. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding PII and PHI, diagnosis of certain conditions, and treatment/medication for such conditions. Furthermore, Defendant intercepted the "contents" of Plaintiffs' communications in at least the following forms:

a. The parties to the communications;

b. Personally, identifying information such as patients' IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;

d. The precise text of patient communications about specific treatments;

e. Information that informs third parties of the general subject of communications that Defendant sends back to patients in response to requests for information about specific conditions, treatments, and diagnosis.

239. Interception. The ECPA defines the 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).

240. Electronical, Mechanical or Other Device. The ECPA defines "electronic, mechanical, 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 Pixel code deployed by Defendant to effectuate the sending and acquisition of patient communications.

241. By utilizing and embedding the Pixels on its Website, 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).

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

243. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding PII and PHI, including their sensitive medical conditions, first and last names, emails, phone numbers, and zip codes.

244. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to affiliates and 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).

245. 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).

246. Unauthorized Purpose. 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, negligence, among others.

247. The ECPA provides that a "party to the communication" may be liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

248. Defendant is not a party for purposes to the communication based on its unauthorized duplication and transmission of communications with Plaintiffs and the Class. However, even assuming Defendant is a party, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiffs' and Class Members' Private Information does not qualify for the party exemption.

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

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

250. Plaintiffs' and Class Members' information that Defendant disclosed to third parties qualifies as IIHI, and Defendant violated Plaintiffs' expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant intentionally used the wire or electronic communications to intercept Plaintiffs Private Information in violation of the law.

251. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it: Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and disclosed individually identifiable health information to Facebook without patient authorization.

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

253. Defendant's acquisition of patient communications that were used and disclosed to Facebook was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and individual States nationwide as set forth herein, including:

a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;
b. Negligence;
c. Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. 505/1, *et seq.*;
d. Illinois Eavesdropping Statute, 720 Ill. Comp. Stat. 5/14, *et seq*.

254. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs' and Class Members' communications about their Private Information on its Webpage, because it used its participation in these communications to improperly share Plaintiff's and Class Members' Private Information with Facebook and third-parties that did not participate in these communications, that Plaintiffs and Class Members did not know was receiving their information, and that Plaintiffs and Class Members did not consent to receive this information

255. As such, Defendant cannot viably claim any exception to ECPA liability.

256. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

e. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their PII and PHI (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiffs and Class Members to suffer emotional distress;

f. Defendant received substantial financial benefits from its use of Plaintiffs' and the Class Members' PII and PHI without providing any value or benefit to Plaintiffs or Class Members;

g. Defendant received substantial, quantifiable value from its use of Plaintiffs' and the Class Members' PII and PHI, such as understanding how people use its Website and determining what ads people see on its Website, without providing any value or benefit to Plaintiffs or Class Members;

h. Defendant has failed to provide Plaintiffs and Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and

i. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, medical treatment, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

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

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

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

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

261. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing

intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

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

COUNT II

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

263. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

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

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

266. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

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

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

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

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

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

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

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

274. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information;

d. Failing to detect in a timely manner that Plaintiffs' and Class Members' Private Information had been compromised; and

e. Failing to timely notify—or notify at all—Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

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

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

277. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner. Therefore, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

COUNT III

VIOLATIONS OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT 815 Ill. Comp. Stat. 505/1, *et seq.*

(*On Behalf of Plaintiffs Cook, Smith and Schoon & the Illinois Subclass*)

278. Plaintiffs Joshua Cook, Jasmine Smith and Melody Schoon repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

279. Defendant is a "person" as defined by 815 ILCS § 505/1.

280. Plaintiffs and the Class Members are "consumers" as defined by 815 ILCS § 505/1.

281. Defendant's unfair acts and practices against Plaintiffs and the Class Members occurred in the course of trade or commerce in Illinois, arose out of transactions that occurred in Illinois, and/or harmed individuals in Illinois.

282. Plaintiffs and the Class Members received and paid for health care services from Defendant.

283. Plaintiffs and the Class Members used Defendant's Website in connection with receiving health care services from Defendant.

284. Plaintiffs' and the Class Members' payments to Defendant for health care services were for household and personal purposes.

285. Defendant's practices of disclosing Plaintiffs' and the Class Members' PII and PHI by re-directing confidential communications via the Meta Pixel to third parties without authorization, consent, or knowledge of Plaintiffs and the Class Members is a deceptive, unfair, and unlawful trade act or practice, in violation of 815 ILCS § 505/2.

286. Defendant's unfair business practices were targeted at all of Defendant's customers, including Plaintiffs and the Class Members.

287. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the privacy, security, and use of their personally identifiable patient data and communications when using Defendant's Website.

288. Defendant intended to mislead Plaintiffs and the Class Members and to induce them to rely on its misrepresentations and omissions.

289. Defendant's surreptitious collection and disclosure of Plaintiffs' and the Class Members' PII, PHI, and communications to third parties involves important consumer protection concerns.

290. Furthermore, the Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/20, provides that a violation of that statute constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* ("ICFA").

291. Defendant is a "data collector" under IPIPA.[57] As a data collector, Defendant owns or licenses information concerning Illinois residents.

292. IPIPA protects Medical Information and Personal Information.[58]

293. The IPIPA requires a data collector that "maintains or stores . . . records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."[59]

294. IPIPA's rights are not subject to waiver.[60]

---

[57] 815 ILL. COMP. STAT. 530/5.

[58] *Id.*

[59] 815 ILL. COMP. STAT. 530/45(a).

[60] 815 ILL. COMP. STAT. 530/15.

295. Defendant represented that it would safeguard and protect Plaintiffs' and Class Members' Private Information, in its Privacy Practices and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

296. Defendant made these representations with the intent to induce Plaintiffs and Class Members to seek health care services from Defendant and to use Defendant's Website in doing so.

297. Plaintiffs and Class Members relied upon Defendant's representations in seeking health care services from Defendant and in using Defendant's Website to obtain such services.

298. The IPIPA further requires that data collectors "notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most *expedient* time possible and *without unreasonable delay*, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system."[61]

299. As alleged above, Defendant violated the IPIPA by failing to implement and maintain reasonable security measures to protect Plaintiffs and Class Members' PHI and PII. Defendant further violated the IPIPA by failing to give Plaintiffs and Class Members expedient notice without unreasonable delay.

300. As a direct and proximate cause of Defendant's unfair acts and practices, Plaintiffs and Class members have suffered actual damages.

301. Plaintiffs' and the Class Members' injuries were proximately caused by Defendant's unfair and deceptive business practices.

[61] 815 ILL. COMP. STAT. 530/10 (emphasis added).

302. As a result of Defendant's conduct, Defendant has been unjustly enriched.

303. Defendant's acts caused substantial injury that Plaintiffs and the Class Members could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

304. Defendant acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiffs' and the Class Members' rights.

305. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive acts and practices, Plaintiffs and the Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including overpaying for Defendant's health care services and loss of value of their personally identifiable patient data and communications.

306. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive acts and practices, Plaintiffs and the Class Members were also damaged by Defendant's conduct in that:

a. Defendant harmed Plaintiffs' and Class Members' interest in privacy;
b. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private has been disclosed to third parties;
c. Defendant eroded the essential confidential nature of the provider-patient relationship;
d. Defendant took something of value from Plaintiffs and Class Members, i.e., their personally identifiable patient information, and derived a benefit therefrom without Plaintiffs' or the Class Members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;
e. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and
f. Defendant's actions diminished the value of Plaintiffs' and Class Members' personal information.

307. As a direct and proximate result of Defendant's above-described violation of the IPIPA and ICFA, Plaintiffs and Class Members are entitled to recover actual damages, reasonable attorneys' fees, and costs.

COUNT IV

VIOLATIONS OF THE ILLINOIS EAVESDROPPING STATUTE
720 Ill. Comp. Stat. 5/14, *et seq*.
(*On Behalf of Plaintiffs Cook, Smith and Schoon & the Illinois Subclass*)

308. Plaintiffs Joshua Cook, Jasmine Smith and Melody Schoon repeat the allegations contained in the foregoing paragraphs as if fully set forth herein.

309. The Eavesdropping Article of the Illinois Criminal Code (the "Illinois Eavesdropping Statute" or "IES") states that it is a felony for any person to knowingly and intentionally "use[] an eavesdropping devise, in a surreptitious manner, for the purpose of transmitting or recording all or part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation."[62]

310. The IES also states that it is a felony for any person to knowingly and intentionally "use[] or disclose[] any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication in violation of this Article, unless he or she does so with the consent of all of the parties."[63]

311. For purposes of the IES, "eavesdropping device" means "any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications

[62] 720 ILL. COMP. STAT. 5/14-2(a), -4.

[63] *Id.*

whether such conversation or electronic communication is conducted in person, by telephone, or by any other means."[64]

312. For purposes of the IES, "surreptitious" means "obtained or made by stealth or deception, or executed through secrecy or concealment."[65]

313. For purposes of the IES, "private electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation. . . . Electronic communication does include any communication from a tracking device."[66]

314. "A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution."[67]

315. Defendant intentionally recorded and/or acquired Plaintiffs' and Class Members' private electronic communications, without the consent of Plaintiffs and Class Members, using the Meta Pixel and similar tracking technologies on its Website.

316. Defendant intentionally recorded and/or acquired Plaintiffs' and Class Members' private electronic communications for the purpose of disclosing those communications to third

[64] 720 ILL. COMP. STAT. 5/14-1(a).

[65] 720 ILL. COMP. STAT. 5/14-1(g).

[66] 720 ILL. COMP. STAT. 5/14-1(e).

[67] *Id.*

parties, including Facebook and Google, without the knowledge, consent, or written authorization of Plaintiffs or Class Members.

317. Plaintiffs' and Class Members' communications with Defendant constitute private conversations, communications, and information.

318. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Website.

319. Plaintiffs and Class Members communicated sensitive PHI and PII that they intended for only Defendant to receive and that they understood Defendant would keep private.

320. Plaintiffs and Class Members have a reasonable expectation that Defendant would not disclose PII, PHI, and confidential communications to third parties without Plaintiffs' or Class Members' authorization, consent, or knowledge.

321. Plaintiffs and Class Members had a reasonable expectation of privacy given Defendant's representations, Notice of Privacy Practices, Terms of Use, and HIPAA. Moreover, Plaintiffs and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

322. Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously recorded and transmitted to third parties as they communicated with Defendant through its Website.

323. Without Plaintiffs' or Class Members' knowledge, authorization, or consent, Defendant used the Meta Pixel imbedded and concealed into the source code of its Website to secretly record and transmit Plaintiffs' and Class Members' private communications to hidden third parties, such as Facebook and Google.

324. Under the IES, "[a]ny or all parties to any conversation or electronic communication upon which eavesdropping is practices contrary to this Article shall be entitled to the following remedies: (a) [t]o an injunction by the circuit court prohibiting further eavesdropping by the eavesdropper and by or on behalf of his principal, or either; (b) [t]o all actual damages against the eavesdropper or his principal or both; [t]o any punitive damages which may be awarded by the court or by a jury. . . ."[68]

325. The eavesdropping devices used in this case include, but are not limited to:

a. Plaintiffs' and Class Members' personal computing devices;
b. Plaintiffs' and Class Members' web browsers;
c. Plaintiffs' and Class Members' browser-managed files;
d. Facebook's Pixel;
e. Internet cookies;
f. Defendant's computing servers;
g. Third-party source code utilized by Defendant; and
h. Computer servers of third-parties (including Facebook) to which Plaintiffs' and Class Members' communications were disclosed.

326. The eavesdropping devices outlined above are not excluding "tracking devices" as that term is used in the IES, 720 ILCS 5/14-1(e), to the extent that they perform functions other than collection of geo-locational data.[69]

327. Defendant is a "person" under the IES.[70]

328. Defendant aided in the interception of communications between Plaintiffs and Class Members and Defendant that were redirected to and recorded by third parties without Plaintiffs' or Class Members' consent.

---

[68] 720 ILL. COMP. STAT. 5/14-6.

[69] *See Vasil v. Kiip, Inc.*, No. 16-cv-9937, 2018 U.S. Dist. LEXIS 35573, at *20-25 (N.D. Ill. Mar. 5, 2018).

[70] 720 ILL. COMP. STAT. 5/2-15.

329. Under the IES, Plaintiffs and the Class Members are entitled to injunctive relief prohibiting further eavesdropping by Defendant, actual damages, and punitive damages.

330. Defendant's breach caused Plaintiffs and Class Members the following damages:

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;
b. Defendant eroded the essential confidential nature of the physician-patient relationship;
c. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value;
d. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and
e. Defendant's actions diminished the value of Plaintiffs' and Class Members' personal information.

331. Plaintiffs and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

COUNT V
VIOLATIONS OF THE NEVADA DECEPTIVE TRADE PRACTICES ACT
NRS Ch. 598
(*On Behalf of Plaintiff Shandari Bush & the Nevada Subclass*)

332. Plaintiff Shandari Bush repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

333. Defendant engaged in unfair and unlawful acts and trade practices by failing to maintain adequate procedures to avoid disclosure of Plaintiff Bush's and Nevada Subclass Members' Private Information and permitting access to this Private Information by the Pixel Information Recipients.

334. Plaintiff Bush and Nevada Subclass members relied on Defendant's implied promise of data privacy and security when providing their Private Information to Defendant.

335. The Nevada Deceptive Trade Practices Act ("NDTPA"), codified in NRS Chapter

598, prohibits unfair and deceptive trade practices in the course of any business or occupation.

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

337. By reason of the conduct alleged herein, Defendant knowingly engaged in unlawful trade practices within the meaning of the NDTPA. Defendant's conduct alleged herein is a "trade practice" within the meaning of the NDTPA, and the deception occurred within the State of Nevada.

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

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

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

341. Defendant's conduct violated NRS 598.0917(7) because it constituted a tender of "goods advertised for sale . . . or tendering terms of sale or lease less favorable than the terms advertised," i.e.:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;
b.
c. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Bush's and Nevada Subclass Members' Private Information from unauthorized disclosure;

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

e.

f. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Bush's and Nevada Subclass Members' Private Information from unauthorized disclosure;

g.

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

i.

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

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

343. Such acts by Defendant are and were deceptive trade practices which are and/or were likely to mislead a reasonable consumer by providing his or her Private Information to Defendant. The requests for and use of such Private Information in Nevada through deceptive means were consumer-oriented acts and thereby fall under the NDTPA.

344. Defendant's violations of NRS 598.0917(7) constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

345. Defendant also breached its duty under NRS 603A.210, which requires any data collector "that maintains records which contain personal information" of Nevada residents to "implement and maintain reasonable security measures to protect those records from unauthorized

access, acquisition, . . . use, modification or disclosure." Defendant did not take such reasonable security measures, instead enabling the Pixel Information Recipients to access Plaintiff's and Nevada Subclass Members' Private Information without authorization or consent.

346. Additionally, NRS 598.0923(3) provides that a violation of any federal or Nevada law constitutes consumer fraud. Thus, Defendant's failure to secure its clients' Private Information which violated the FTCA, NRS 598.0917(7), and NRS 603A, is a violation of NRS 598.0923(3).

347. Defendant's violations of NRS 598.0923(3) constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

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

349. Defendant's violations of the NDTPA have an impact and general importance to the public, including the people of Nevada. Thousands of Nevada citizens have had their Private Information transmitted without consent from Defendant's Website to third parties.

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

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

COUNT VI

VIOLATIONS OF THE MARYLAND WIRETAP ACT
Md. Code Ann., Cts. & Jud. Proc. § 10-402
(*On Behalf of Plaintiff Reedy & the Maryland Subclass*)

352. Plaintiff Ashley Reedy repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

353. The Maryland Wiretap Act (the "Act") prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the willful disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the willful use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. Md. Code Ann., Cts. & Jud. Proc. § 10-402.

354. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. Md. Code Ann., Cts. & Jud. Proc. § 10-410(a).

355. Defendant qualifies as a person under the Act because it is a corporation. *See* Md. Code Ann., Cts. & Jud. Proc. § 10-401(14) (defining "[p]erson" as "any individual, partnership, association, joint stock company, trust or corporation."

356. "Intercept" is defined as any "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device."

Md. Code Ann., Cts. & Jud. Proc. § 10-401(10).

357. "Contents" is defined as when "used with respect to any wire, oral, or electronic communication, includes any information concerning the identity of the parties to the communication or the existence, substance, purport, or meaning of that communication." Md. Code Ann., Cts. & Jud. Proc. § 10-401(4).

358. "Electronic Communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system." Md. Code Ann., Cts. & Jud. Proc. § 10-401(5)(i).

359. Defendant willfully engaged in and continues to engage in intercepting communications by aiding others (including Facebook) to secretly record the contents of Plaintiff Bush's and Class Members' electronic communications.

360. The intercepting devices in this case include, but are not limited to:

a. Plaintiff's and Maryland Subclass Members' personal computing devices;
b. Plaintiff's and Maryland Subclass Members' web browsers;
c. Plaintiff's and Maryland Subclass Members' browser-managed files;
d. Facebook's Meta Pixel;
e. Internet cookies;
f. Defendant's computer servers;
g. Third-party source code utilized by Defendant; and
h. Computer servers of third parties (including Facebook) to which Plaintiff's and Maryland Subclass Members' communications were disclosed.

361. Defendant willfully aided in, and continues to aid in, the interception of contents in that data from the communications between Plaintiff and/or Maryland Subclass Members and Defendant that were redirected to and recorded by the third parties include information which identifies the parties to each communication, their existence, and their contents.

362. The Defendant aided in the interception of "contents" in at least the following

forms:

a. The parties to the communications;
b. PII such as Plaintiff's and Maryland Subclass Members' IP addresses, Facebook IDs, browser fingerprints and other unique identifiers;
c. The precise names of sensitive tests viewed, added to cart and/or purchased by Plaintiff and Maryland Subclass Members;
d. The precise text of buttons clicked by Plaintiff and Maryland Subclass Members;
e. Plaintiff's and Maryland Subclass Members' sensitive medical conditions and medical tests sought;
f. The dates and times when Plaintiff and Maryland Subclass Members accessed the Website, including when they logged into their account with Defendant;
g. Descriptive information about the webpages visited by Plaintiff and Maryland Subclass Members including the title of the webpage;
h. Information that is a general summary or informs third parties of the general subject of communications that Defendant sends back to customers in response to search queries and requests for information about specific medical conditions, treatments, and medical tests sought;
i. Any other content that Defendant has aided third parties in scraping from its webpages or communication forms at its Website.

363. Defendant willfully procures and embeds the Meta Pixel (and other tracking codes) on its Website to spy on, automatically and secretly, and intercept its Website visitors' electronic interactions communications with Everly Well in real time.

364. Plaintiff's and Maryland Subclass Members' electronic communications were/are intercepted contemporaneously with their transmission.

365. Plaintiff and Maryland Subclass Members reasonably expected that their Private Information was not being intercepted, recorded and disclosed to Facebook and other third parties.

366. Plaintiff and Maryland Subclass Members did not consent to having their Website communications, which include their Private Information, wiretapped.

367. No legitimate commercial purpose was served by Defendant's willful and intentional disclosure of Plaintiff's and Maryland Subclass Members' Private Information to Facebook.

368. Plaintiff's and Maryland Subclass Members' electronic communications were

intercepted during transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their Private Information, including using their sensitive medical information to develop marketing and advertising strategies.

369. Pursuant to Md. Code Ann., Cts. & Jud. Proc. § 10-410 Plaintiff and the Maryland Subclass members seek (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

370. Defendant's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Maryland Subclass Members any time they visit Defendant's Website with the Meta Pixel enabled without their consent. Plaintiff and Maryland Subclass Members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

PRAYER FOR RELIEF

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

A. an Order certifying the Nationwide Class and Illinois, Nevada and Maryland Subclasses, and appointing Plaintiffs and their Counsel to represent the Classes;

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

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

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

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

law;

F. prejudgment interest on all amounts awarded and

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

DEMAND FOR JURY TRIAL

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

Dated: April 4, 2024

Respectfully submitted,

/s/ David S. Almeida
David S. Almeida (ARDC No. 6285557)
Matthew J. Langley (ARDC No. 6337129)
Britany Kabakov (ARDC No. 6336126)
ALMEIDA LAW GROUP LLC
849 W Webster Avenue
Chicago, IL 60614
Tel: (312) 576-3024
david@almeidalawgroup.com
matt@almeidalawgroup.com
britany@almeidalawgroup.com

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

**pro hac vice admission anticipated*

Attorneys for Plaintiffs & the Classes