UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

W.W., *on behalf of herself and all others similarly situated*, Plaintiff, v. ORLANDO HEALTH MEDICAL GROUP, INC., Defendant.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff W.W. is a current patient of Orlando Health Medical Group, Inc. ("Orlando Health" or "Defendant"), who brings this class action against Defendant in her individual capacity[1] and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions, her counsels' investigation, and upon information and belief as to all other matters, as follows:

1. Plaintiff brings this case to address Defendant's outrageous, illegal, and widespread practice of disclosing Plaintiff's and Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively

1 Plaintiff brings this action anonymously out of a desire to protect her personal health information under the Health Insurance Portability and Accountability Act of 1996.

referred to as "Private Information") to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook").

2. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace or denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

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

4. Defendant owns and controls www.orlandohealth.com ("Defendant's Website" or the "Website"), which it encourages patients to use for booking medical appointments, locating physicians and treatment facilities, communicating medical

symptoms, searching medical conditions and treatment options, signing up for events and classes, and more.

5. Plaintiff and other Class Members who used Defendant's Website thought they were communicating only with their trusted healthcare provider. Unbeknownst to Plaintiff and Class Members, however, Defendant had embedded the Facebook Tracking Pixel (the "Pixel" or "Facebook Pixel") on its Website, surreptitiously forcing Plaintiff and Class Members to transmit to Facebook every click, keystroke, and intimate detail about their medical treatment. Operating as designed and as implemented by Defendant, the Pixel allows the Private Information that Plaintiff and Class Members submit to Defendant to be unlawfully disclosed to Facebook alongside the individual's unique and persistent Facebook ID ("FID").[2]

6. A pixel is a piece of code that "tracks the people and [the] type of actions they take"[3] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), among other things.

---

[2] The Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023)

[3] Facebook, *Retargeting*, https://www.facebook.com/business/goals/retargeting (last visited Nov. 14, 2022)

7. The user's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Facebook Pixel is thus customizable and programmable, meaning that the website owner controls which of its webpages contain the Pixel and which events are tracked and transmitted to Facebook. By installing the Facebook Pixel on its Website, Defendant effectively planted a bug on Plaintiff and Class Members' web browsers and compelled them to disclose their communications with Defendant to Facebook.

8. The Office for Civil Rights (OCR) at HHS has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[4] The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules." In other words, HHS has expressly stated that entities like Defendant that implement the Facebook Pixel have violated HIPAA Rules.

9. In addition to the Facebook Pixel, Defendant also installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on its Website servers.[5]

---

[4] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Feb. 20, 2023).

[5] "CAPI works with your Facebook pixel to help improve the performance and measurement of

10. Unlike the Facebook Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[6,7] Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[8]

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

12. Defendant utilized the Pixel and CAPI data for marketing purposes in an effort to bolster its profits. The Facebook Pixel and CAPI are routinely used to target

---

your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Jan. 25, 2023).

[6] https://revealbot.com/blog/facebook-conversions-api/ (last visited Jan. 24, 2023).

[7] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels.", https://developers.facebook.com/docs/marketing-api/conversions-api (last visited Jan. 27, 2023).

[8] https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Jan. 28, 2023).

specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff's and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

13. The information that Defendant's Tracking Pixel and CAPI sent to Facebook included the Private Information that Plaintiff and Class Members submitted to Defendant's Website, including for example, the type of medical treatment sought, the individual's particular health condition, and the fact that the individual attempted to or did book a medical appointment.

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

15. Healthcare patients simply do not anticipate that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party – let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue – without the

patients' consent. Neither Plaintiff nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook.

16. Despite willfully and intentionally incorporating the Facebook Pixel and CAPI into its Website and servers, Defendant has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook. Plaintiff and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook as they communicated with their healthcare provider via the Website, or stored on Defendant's servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes.

17. Defendant breached its statutory and common law obligations to Plaintiff and Class Member by, inter alia,: (i) failing to adequately review its marketing programs and web-based technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Facebook Pixels; (v) failing to warn Plaintiff and Class Members; and (vi) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

18. As a result of Defendant's conduct, Plaintiff and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Pixel, (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information, (v) statutory damages, and (v) the continued and ongoing risk to their Private Information.

19. Plaintiff seeks to remedy these harms and brings causes of action for (1) violation of the Florida Security of Communications Act, Florida Statutes § 934.01, *et seq.*; (2) invasion of privacy under Florida's Constitution; (3) invasion of privacy; (4) breach of implied contract; (5) unjust enrichment; (6) violations of the Electronics Communication Privacy Act ("ECPA") 18 U.S.C. § 2511(1) – unauthorized interception, use, and disclosure; (7) violations of ECPA, 18 U.S.C. § 2511(3)(a) – unauthorized interception, use, and disclosure; (8) violations of Title II of the ECPA, 18 U.S.C. § 2702, et seq., - Stored Communications Act; (9) violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, et seq.; and (10) breach of confidence.

PARTIES

Plaintiff W.W.

20. Plaintiff is a natural person and citizen of Florida where she intends to remain. Plaintiff brings this complaint anonymously to protect her personal health information pursuant to HIPAA. On numerous occasions, Plaintiff accessed Defendant's Website on her mobile device and/or computer. Plaintiff used the Website to find and obtain medical treatment. Pursuant to the systematic process described in this Complaint,

Plaintiff's Private Information was disclosed to Facebook, and this data included her PII, PHI, and related confidential information. Defendant intercepted and/or assisted these interceptions without Plaintiff's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff's Private Information.

21. Plaintiff has received healthcare services since 2010 at one of the hospitals in Defendant's network and has used Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

22. Plaintiff has used Defendant's Website for at least the past three to four years.

23. Plaintiff used Defendant's Website to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, review medical records, and review and pay medical bills.

24. Plaintiff has been a Facebook user since at least 2019 and maintains an active account which she uses on a regular basis.

25. Plaintiff accessed Defendant's Website to receive healthcare services from Defendant or Defendant's affiliates, at Defendant's direction, and with Defendant's encouragement.

26. As Defendant's patient, Plaintiff reasonably expected that her online communications with Defendant were solely between herself and Defendant and that such communications would not be transmitted to or disclosed to a third party. But for her status

as Defendant's patient, Plaintiff would not have disclosed her Private Information to Defendant.

27. During her time as a patient, Plaintiff never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information.

28. Notwithstanding, through the Pixel and Conversions API, Defendant transmitted Plaintiff's Private Information to third parties, such as Facebook and Google.

Defendant Orlando Health Medical Group, Inc.

29. Defendant Orlando Health Medical Group, Inc. is headquartered at 1414 Kuhl Avenue, Orlando, FL 32806. Service is proper on its registered agent, Zika Ryan, Esq., located at 207 W. Gore St., Suite 201, Orlando, FL 32806.

30. "Orlando Health is a not-for-profit healthcare organization with $8.1 billion of assets under management that serves the southeastern United States. Headquartered in Orlando, Florida, the system was founded more than 100 years ago."[9] "Orlando Health is a 3,238-bed system that includes 23 hospitals and emergency departments – 18 of which are currently operational with five coming soon. The system also includes nine specialty institutes in aesthetic and reconstructive surgery, cancer, colon and rectal, digestive health, heart and vascular, neuroscience, orthopedics, rehabilitation, weight loss and bariatric surgery."[10] "The Orlando Health system . . . employs more than 25,000 team members and

[9] https://www.orlandohealth.com/about-us (last visited February 24, 2023)
[10] *Id.*

more than 1,200 physicians."[11] "In FY22, Orlando Health served nearly 142,000 inpatients and 3.9 million outpatients."[12]

31. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 (HIPAA)).

JURISDICTION & VENUE

32. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this case is brought as a class action where the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendant.

33. This Court has federal question jurisdiction under 29 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (28 U.S.C. § 2511, *et seq.*, and 28 U.S.C. § 2702) and the CFAA (18 U.S.C. § 1030, *et seq*).

34. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

35. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

[11] *Id.*
[12] *Id.*

COMMON FACTUAL ALLEGATIONS

A. Background: Underlying Technology Employed by Defendant for the Purpose of Disclosing Plaintiff and Class Members' Private Information to Facebook

36. Defendant uses its Website to connect Plaintiff and Class Members to Defendant's digital healthcare platforms with the goal of increasing profitability.

37. In furtherance of that goal, and to increase the success of its advertising and marketing, Defendant purposely installed the Pixel and CAPI tools on many of its webpages within its Website and on its servers and programmed those webpages and servers. In doing so, Defendant surreptitiously shared patients' private and protected communications with Facebook, including communications that contain Plaintiff's and Class Members' Private Information.

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

i. Facebook's Business Tools and the Pixel

39. 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.[13]

[13] Facebook, *Meta Reports Fourth Quarter and Full Year 2021 Results* , https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).

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

41. Facebook's Business Tools, including the Pixel and Conversions API, 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.

42. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[14] Businesses that want to target customers and advertise their services, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[15]

43. One such Business Tool is the Pixel that "tracks the people and type of actions they take."[16] When a user accesses a webpage that is hosting the Pixel, the

---

[14] Facebook, *Specifications for Facebook Pixel Standard Events,* https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Jan. 31, 2023); *see* Facebook, *Facebook Pixel, Accurate Event Tracking, Advanced*, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Facebook, *Best Practices for Facebook Pixel Setup*, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; Facebook, *App Events API*, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Jan. 31, 2023).

[15] Facebook, *About Standard and Custom Website Events*, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* Facebook, *App Events API*, *supra*.

[16] Facebook, *Retargeting*, https://www.facebook.com/business/goals/retargeting.

communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook—traveling from the user's browser to Facebook's server.

44. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate privacy (such as the homepage) and disable it on pages that do implicate patient privacy (such as the "find a doctor" page). Thus, Plaintiff's and Class Member's Private Information would not have been disclosed to Facebook via the Pixel but for Defendant's decisions to install the Pixel on its Website and specifically on the webpages that solicit and receive Private Information.

45. Similarly, Plaintiff's and Class Member's Private Information would not have been disclosed to Facebook via Conversions API but for Defendant's decision to install and implement that tool on its servers.

46. By installing and implementing both tools, Defendant caused Plaintiff's and Class Member's communications to be intercepted and transmitted from Plaintiff's and Class Members' browsers directly to Facebook via the Pixel, or to be recorded on Defendant's servers and then transferred to Facebook via Conversions API. [17]

[17] Facebook assigns a unique "event_id" parameter to each separate communication with a website and then deduplicates the data based on the event_id so that the same event tracked by the Pixel and recorded by the CAPI are not reported as two separate events. https://www.facebook.com/business/help/702509907046774 (last visited Jan. 28, 2023).

ii. Defendant's Method of transmitting Plaintiff's and Class Members' Private Information via the Tracking Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Pixel

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

48. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

49. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses. Any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies[18]:

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

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

a large amount of data outside of the URL (*e.g.*, uploading a PDF to a court's ECF system for filing a motion).

- **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 that have been placed on the client device 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 to the cookie owner's website when the user is visiting 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.[19] HTTP Responses can also send cookies or other code hidden and embedded in the webpage to the client device's browser.

50. When an individual visits Defendant's Website, an HTTP Request is sent from that individual's web browser to Defendant's servers that essentially asks Defendant's Website to retrieve certain information (such as Defendant's "Make an Appointment" page). The HTTP Response from Defendant's servers sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Website.

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

51. Every website is comprised of Markup and "Source Code." Source Code is simply 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.

52. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's customized implementation of the Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When patients visit Defendant's website via an HTTP Request to North Memorial's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user along with Source Code that includes Defendant's Pixel. In essence, Defendant is handing patients a bugged phone. Once the Webpage loads in the patient's browser, the software-based wiretap quietly waits for a communication from the patient to trigger the tap, which intercepts those communications intended only for Defendant and transmits them to third-parties, including Facebook.

53. Separate from the Pixel, Facebook and other website owners can place third-party cookies in the web browsers of users logged into their websites or services. These cookies can uniquely identify the user so the cookie owner can track the user as she moves around the internet – whether on the cookie owner's website or not. Facebook uses this type of third-party cookie when Facebook account holders use the Facebook app or website. As a result, when a Facebook account holder uses Defendant's Website, a unique

id is sent to Facebook along with the intercepted communication that allows Facebook to identify the patient associated with the Private Information it has intercepted.

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

55. Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]." Thus, Defendant receives and stores its communications with patients on its server before Conversions API collects and sends those communications—and the Private Information contained therein—to Facebook.

56. Notably, client devices do not have access to host servers and thus cannot prevent (or even detect) this additional transmission of information to Facebook.

57. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the host server, Facebook instructs companies like Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[20] Thus, since Defendant

[20] *See* https://www.facebook.com/business/help/308855623839366?id= 818859032317965 (last

implemented the Pixel in accordance with Facebook's documentation, it is also reasonable to infer that Defendant implemented the Conversions API tool on its website.

58. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content on the host website. In other words, Facebook and others like it are not providing anything to the user relating to the user's communications. Instead, these third parties are typically procured to track user data and communications only to serve the marketing purposes of the website owner (*i.e.,* to bolster profits).

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

60. In this case, Defendant employed the Pixel and Conversions API to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook.

61. For example, when a patient visits www.orlandohealth.com and selects the "Find a Physician" button, the patient's browser automatically sends an HTTP Request to Defendant's web server, which automatically returns an HTTP Response and loads the Markup for that particular webpage as depicted below.

visited Jan. 23, 2023).

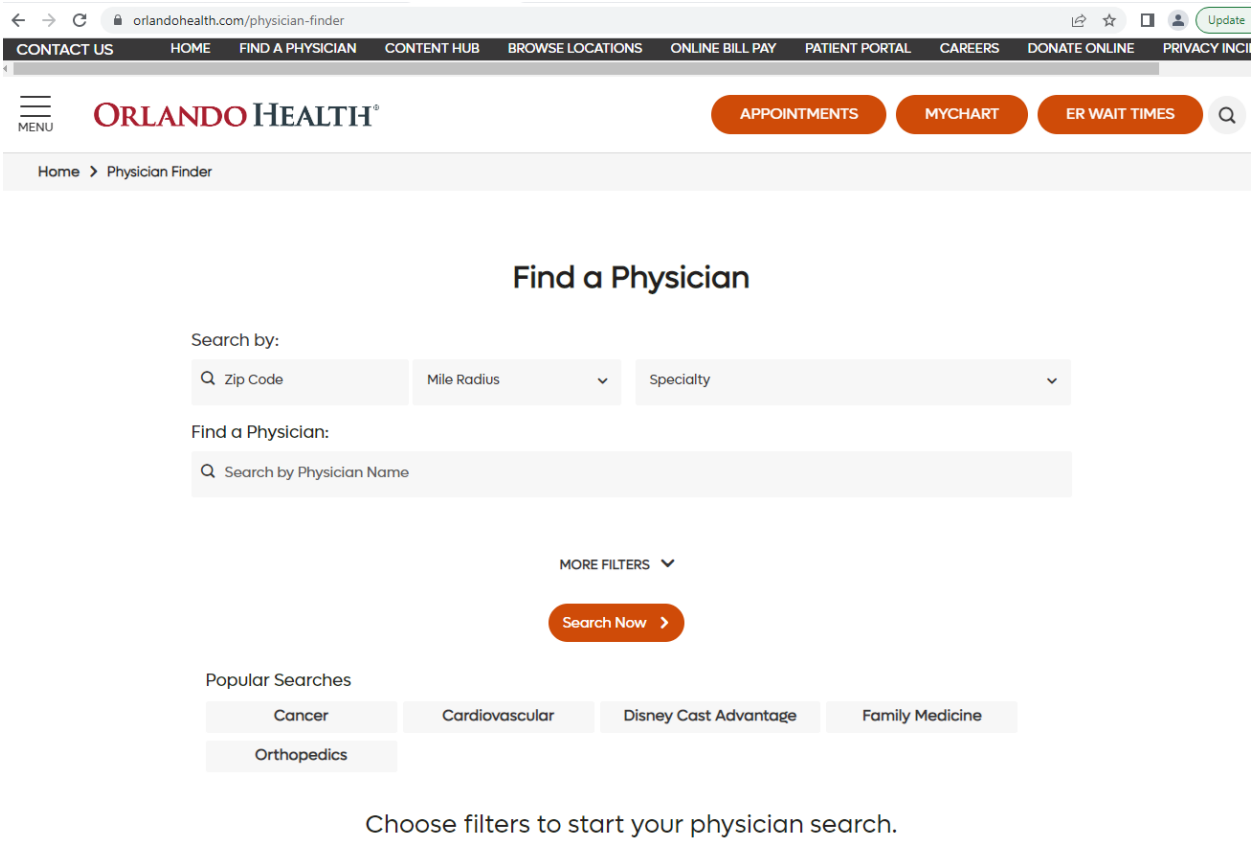


Figure 1. The image above is a screenshot taken from the user's web browser upon visiting https://orlandohealth.com/physician-finder (last accessed Feb. 24, 2023), which depicts the "mark up" or forward facing portion of the website.

62. The patient visiting this particular web page only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

63. The Facebook Tracking Pixel is embedded in Defendant's Source Code contained in its HTTP Response. The Pixel, programmed to automatically track and transmit the patient's communications with Defendant's Website to Facebook, executes instructions that effectively open a hidden spying window into the patient's browser

through which Facebook can intercept the visitor's data, actions, and communications with Defendant.[21]

64. Thus, Defendant's Source Code containing the Pixel manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and sends the communications to Facebook.

65. This communication to Facebook occurs contemporaneously, invisibly, and without the patient's knowledge.

66. Thus, without its patients' consent, Defendant has effectively used its source code to commandeer and "bug" or "tap" patients' computing devices, allowing Facebook to listen in on all of their communications with Defendant and thereby intercept those communications, including Private Information.

67. Consequently, when Plaintiff and Class Members visit Defendant's website and communicate their Private Information, including, but not limited to, medical treatment sought, appointment type, selected physician's name and specialty, specific button/menu selections, content (such as searches for symptoms or treatment options) typed into free text boxes, and demographic information, it is simultaneously intercepted and transmitted to Facebook.

[21] When used in the context of a screen or visual display, a "pixel" is the smallest unit in such a digital display. An image or video on a device's screen can be made up of millions of individual pixels. The Facebook Pixel is a tiny image file that is so small as to be invisible to website users. It is purposefully designed and camouflaged in this manner so that website users remain unaware of it.

B. Defendant Disclosed Plaintiff's and Class Members' Private Information to Facebook Using the Pixel and/or Conversions API Tracking Practices

68. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel and Conversions API on its Website and servers to secretly track patients by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties and obligations.[22]

69. Defendant's Pixel has its own unique identifier (represented as id=816179185220316), which can be used to identify which of Defendant's webpages contain the Pixel.

70. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs.[23] However, Defendant's Website does not rely on the Pixel in order to function.

71. While seeking and using Defendant's services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendant via its Website.

72. Plaintiff and Class Members were not aware that their Private Information would be shared with Facebook as it was communicated to Defendant because, amongst other things, Defendant did not disclose this fact.

73. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to Facebook, nor did

[22] *Id.*

[23] *Id.*

they intend for Facebook to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

74. Defendant's Pixel and Conversions API sent non-public Private Information to Facebook, including but not limited to Plaintiff's and Class Members': (1) status as medical patients; (2) health conditions; (3) desired medical treatment or therapies; (4) appointment requests; (5) desired locations or facilities where treatment was sought; and (6) phrases and search queries (such as searches for symptoms, treatment options, or types of providers) conducted via the general search bar.

75. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside the Plaintiff's and Class Members' Facebook ID (c_user cookie or "FID"), thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts and therefore their identity.[24]

76. 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 ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

[24] Defendant's Website track and transmit data via first-party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

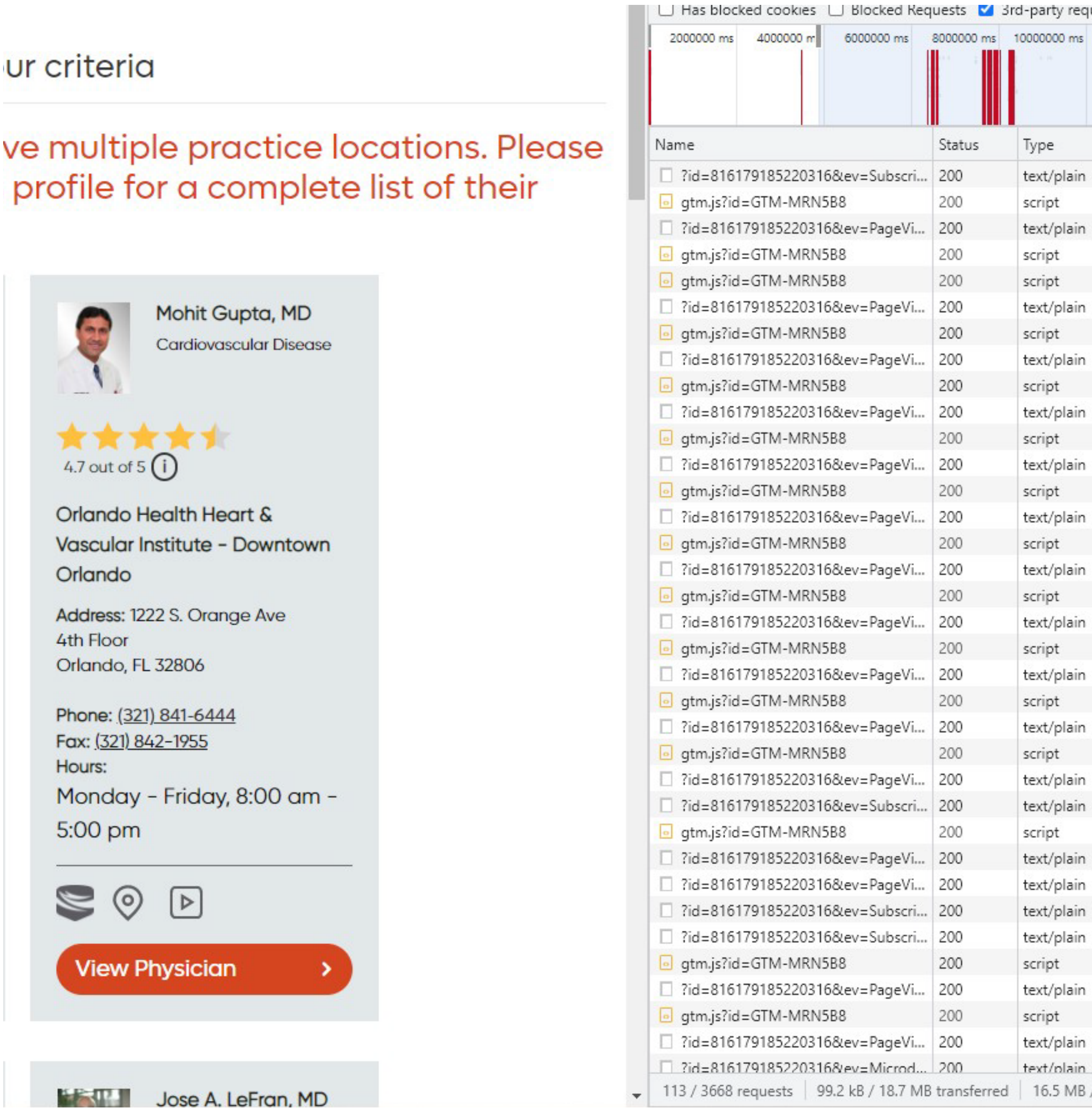
77. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (i.e., the Facebook Pixel and Conversions API) that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Facebook—an unauthorized third-party; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

i. Defendant's Pixel Disseminates Patient Information via Its Website

78. An example illustrates the point. If a patient uses orlandohealth.com to book an appointment with a cardiologist, Defendant's Website directs them to communicate Private Information. Unbeknownst to the patient, each and every communication is sent to Facebook via Defendant's Pixel, including the medical condition the patient types into the search bar and the filters they select.

79. In the example below, the user searched for a physician specialized in treating "cardiovascular disease" who identifies as "Male," speaks "Spanish," is based in "Orlando," and is currently offering "Online Scheduling."

80. Unbeknownst to ordinary patients, the webpage—which is undoubtedly used to communicate Private Information for the purpose of seeking medical treatment—contains Defendant's Pixel. The image below shows the "behind the scenes" portion of the website that is invisible to ordinary users. Importantly, each entry in the column represents just one instance in which Defendant's Pixel sent the user's information to Facebook.



81. Thus, without alerting the user, Defendant's Pixel sends each and every communication the user made via the webpage to Facebook, and the images below confirm

that the communications Defendant sends to Facebook contain the user's Private Information.

82. The next image shows what information is sent to Facebook when the patient selects Dr. Jose A. LeFran's physician profile page and subsequently clicks the "Online Scheduling" button.

83. The first line of highlighted text, "tr/?id=816179185220316," refers to Defendant's Pixel ID and confirms that Defendant has downloaded the Pixel into its Source Code for this particular webpage.

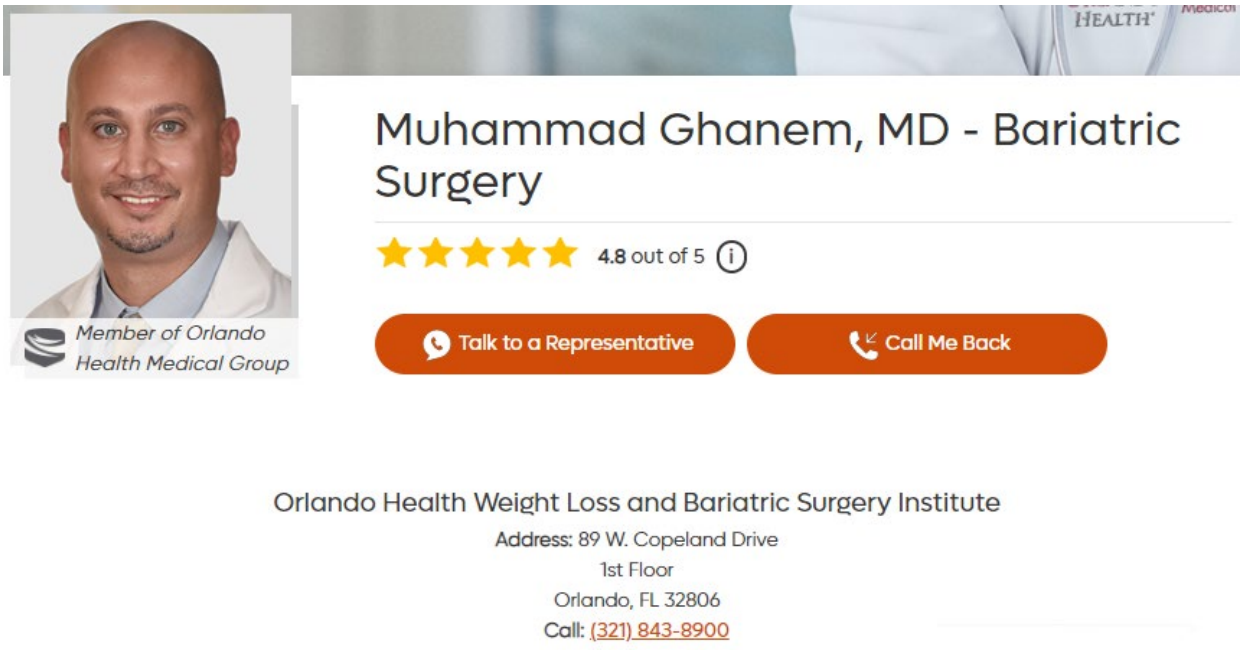
84. The second line of text, "ev: SubscribedButtonClick," identifies and categorizes which actions the user took on the Webpage ("ev:" is an abbreviation for event, and "SubscribedButtonClick" is the type of event). Thus, this identifies the user as having viewed the particular webpage after applying their search criteria, and it also identifies them as having clicked the "Online Scheduling" button.

85. The next lines of highlighted text show Defendant has disclosed to Facebook that the user: (1) is a patient seeking medical care from Defendant via orlandohealth.com; (2) in conjunction with a specific medical condition (highlighted above as "Specialty Cardiovascular Disease"); and (3) is in the process of booking an appointment or searching for a particular physician ("physician-finder" and "Has Online Scheduling") who speaks Spanish ("Languages Spanish"), is based in Orlando ("City Orlando"), and is male ("Gender Male").

86. The text also reveals the identity of the user's physician or perspective physician (highlighted above as "jose-a-lefran-md"), the physician's particular field of medicine or specialty ("Orlando Cardiologist" and "Cardiovascular Disease Doctor"), and the fact that the user scheduled or attempted to schedule an appointment with Dr. Jose A. LeFran ("[buttonText]=Online Scheduling;" '[buttonFeatures]=schedule_button;" and "destination . . . physician-finder . . . jose-a-lefran-md . . . scheduling").

87. Finally, the highlighted text ("GET") combined with the user's Facebook ID (highlighted as "c_user=" in the image above) demonstrates that Defendant's Pixel sent the user's communications, and the Private Information contained therein, alongside the user's Facebook ID (c_user ID), thereby allowing the user's communications and actions on the website to be linked to their specific Facebook profile.[25]

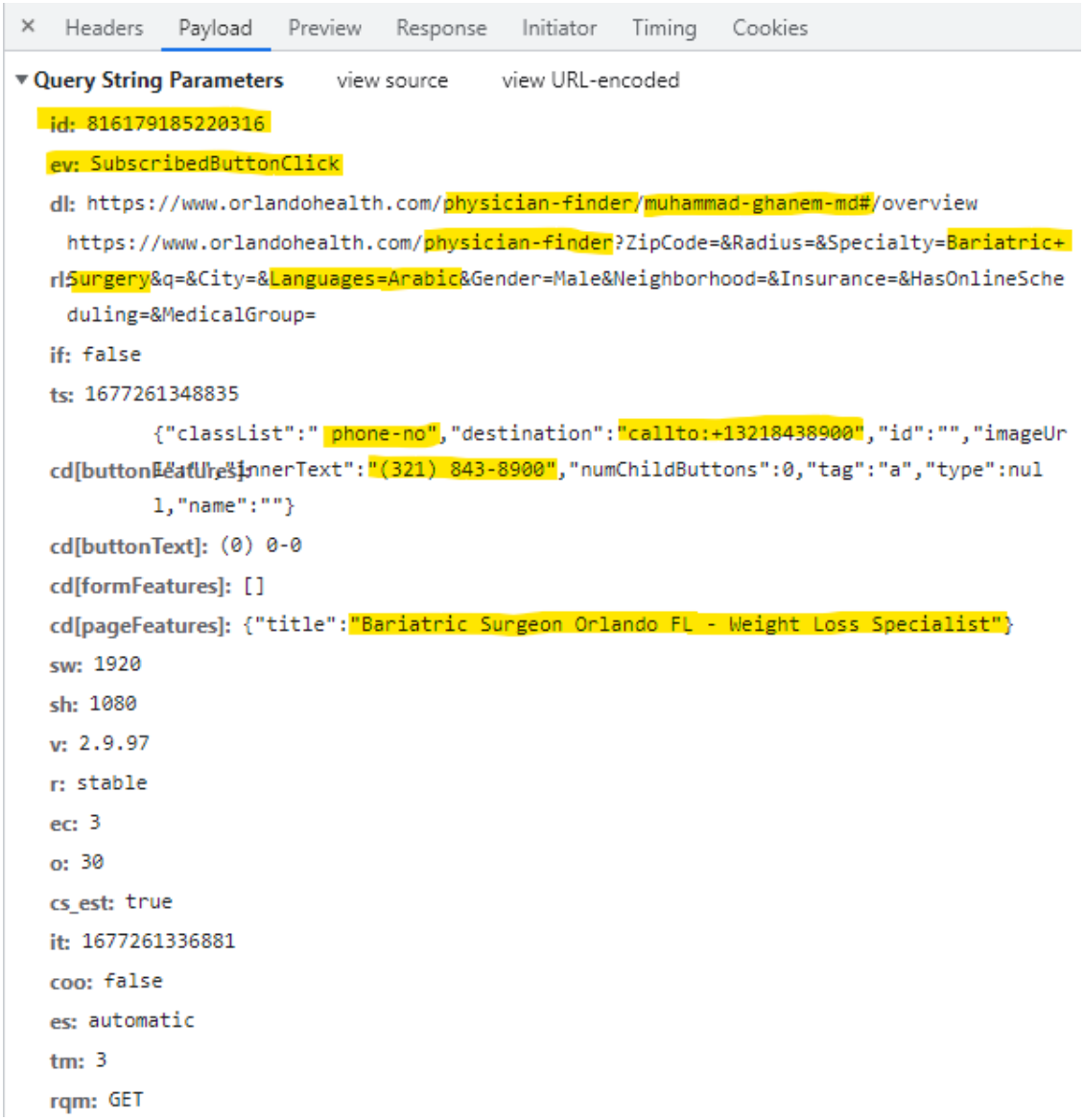
88. Defendant's pixel also tracks and records instances in which a patient or prospective patient has called or attempted to call their physician's phone number from the website in conjunction with their scheduling request. For example, the images below shows the information Defendant communicates to Facebook when a user attempts to call Dr. Muhammad Ghanem's office by clicking the link on his physician profile page.



[25] The user's Facebook ID is represented as the c_user ID highlight in the image above, and Plaintiff has redacted the corresponding string of numbers to preserve the user's anonymity.

89. As with the previous example, the user's search parameters and filters are communicated to Facebook via Defendant's pixel, and their phone call (or attempted phone call) is recorded as a "SubscribedButtonClick."

90. In this example, the user was searching for a "Male" physician, specialized in "Bariatric Surgery," who speaks "Arabic." The text not only reveals the fact that the user called or attempted to call their physician's office, it also reveals the physician's identity ("physician finder" and "muhammad-ghanem-md#"), his specialty ("Specialty=Bariatric+ Surgery" and "Bariatric Surgeon Orlando FL – Weight Loss Specialist"); and the phone number ("phone-no", "destination": "callto:+13218438900").



× Headers Payload Preview Response Initiator Timing Cookies

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

id: 816179185220316

ev: SubscribedButtonClick

dl: https://www.orlandohealth.com/physician-finder/muhammad-ghanem-md#/overview

rl: https://www.orlandohealth.com/physician-finder?ZipCode=&Radius=&Specialty=Bariatric+Surgery&q=&City=&Languages=Arabic&Gender=Male&Neighborhood=&Insurance=&HasOnlineScheduling=&MedicalGroup=

if: false

ts: 1677261348835

cd[buttonFeatures]: {"classList":" phone-no","destination":"callto:+13218438900","id":"","imageUrl":"","innerText":"(321) 843-8900","numChildButtons":0,"tag":"a","type":null,"name":""}

cd[buttonText]: (0) 0-0

cd[formFeatures]: []

cd[pageFeatures]: {"title":"Bariatric Surgeon Orlando FL - Weight Loss Specialist"}

sw: 1920

sh: 1080

v: 2.9.97

r: stable

ec: 3

o: 30

cs_est: true

it: 1677261336881

coo: false

es: automatic

tm: 3

rqm: GET

▼ Request Headers

:authority: www.facebook.com

:method: GET

:path: /tr/?id=816179185220316&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.orlandohealth.com%2Fphysician-finder%2Fmuhammad-ghanem-md%23%2Foverview&rl=https%3A%2F%2Fwww.orlandohealth.com%2Fphysician-finder%3FZipCode%3D%26Radius%3D%26Specialty%3DBariatric%2BSurgery%26q%3D%26City%3D%26Languages%3DArabic%26Gender%3DMale%26Neighborhood%3D%26Insurance%3D%26HasOnlineScheduling%3D%26MedicalGroup%3D&if=false&ts=1677261348835&cd[buttonFeatures]=%7B%22classList%22%3A%22%20phone-no%22%2C%22destination%22%3A%22callto%3A%2B13218438900%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22(321)%20843-8900%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22%3A%22%22%7D&cd[buttonText]=(0)%200-0&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22Bariatric%20Surgeon%20Orlando%20FL%20-%20Weight%20Loss%20Specialist%22%7D&sw=1920&sh=1080&v=2.9.97&r=stable&ec=3&o=30&cs_est=true&it=1677261336881&coo=false&es=automatic&tm=3&rqm=GET

:scheme: https

accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

accept-encoding: gzip, deflate, br

accept-language: en-US,en;q=0.9

cookie: sb=VrLBY5y36a3RDUuvDZHMHwFK; datr=VrLBYwe38VyhLPXyBwHdGCHz; c_user=[redacted] xs=16%3Adc-OmvjWvJCxQw%3A2%3A1673890850%3A-1%3A2663%3A%3AAcXT-b0D8pSknXzTbqrLu6AWiLQikeY4FJ5vjr9gcoo; fr=0JqUksNd1LHSOalxC.AWUiyN9CBAP0WsGsuUDauUJVnWo.Bj-M94.IK.AAA.0.0.Bj-M94.AWXyiYwxgGY

referer: https://www.orlandohealth.com/

sec-ch-ua: "Not_A Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

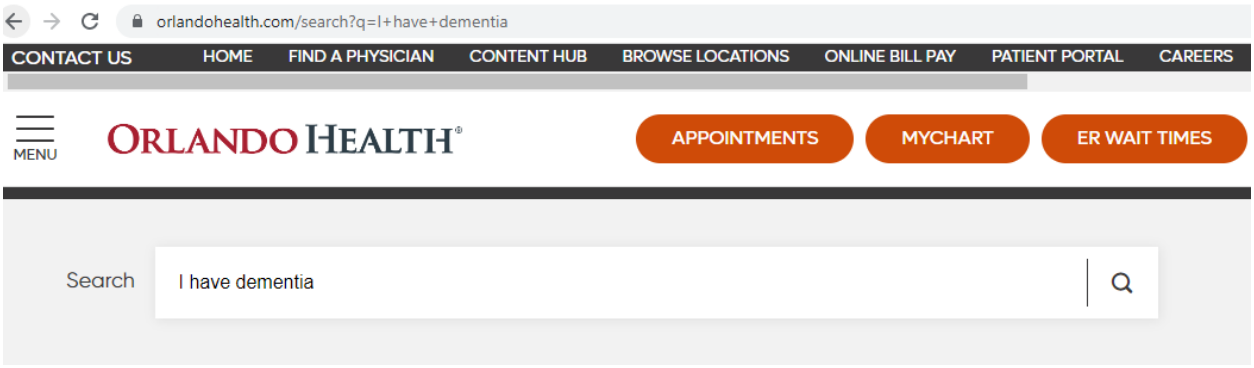
sec-fetch-dest: image

sec-fetch-mode: no-cors

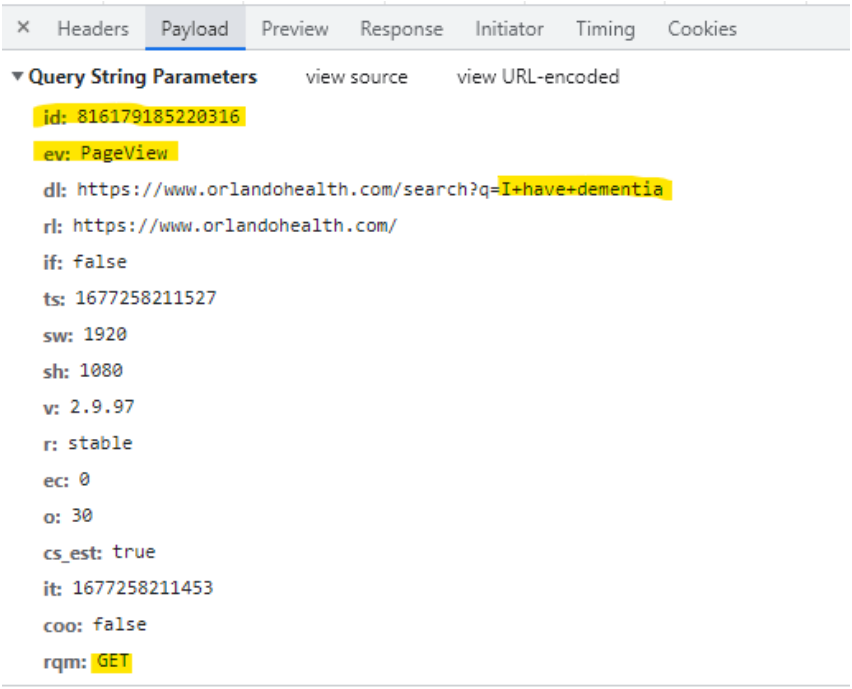
sec-fetch-site: cross-site

user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36

91. To make matters worse, Defendant's Pixel even tracks and records the exact text and phrases that a user types into the general search bar located on Defendant's homepage, orlandohealth.com.



92. In the example above, the user typed "I have dementia" into the search bar, and Defendant's Pixel sent that exact phrase to Facebook, thereby allowing the user's medical condition to be linked to their individual Facebook account for future retargeting and exploitation. This is simply unacceptable, and there is no legitimate reason for sending this information to Facebook.



▼ Request Headers

:authority: www.facebook.com

:method: GET

:path: /tr/?id=816179185220316&ev=PageView&dl=https%3A%2F%2Fwww.orlandohealth.com%2Fsearch%3Fq%3DI%2Bhave%2Bdementia&rl=https%3A%2F%2Fwww.orlandohealth.com%2F&if=false&ts=1677258211527&sw=1920&sh=1080&v=2.9.97&r=stable&ec=0&o=30&cs_est=true&it=1677258211453&coo=false&rqm=GET

:scheme: https

accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

accept-encoding: gzip, deflate, br

accept-language: en-US,en;q=0.9

cookie: sb=VrLBY5y36a3RDUuvDZHMHwFK; datr=VrLBYwe38VyhLPXyBwHdGCHz; c_user=[redacted] xs=16%3Adc-OmvjWvJCxQw%3A2%3A1673890850%3A-1%3A2663%3A%3AAcXT-b0D8pSknXzTbqrLu6AWiLQikeY4FJ5vjr9gcoo; fr=0JqUksNd1LHSOalxC.AWUiyN9CBAP0WsGsuUDauUJVnWo.Bj-M94.IK.AAA.0.0.Bj-M94.AWXyiYwxgGY

referer: https://www.orlandohealth.com/

sec-ch-ua: "Not_A Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

sec-fetch-dest: image

sec-fetch-mode: no-cors

sec-fetch-site: cross-site

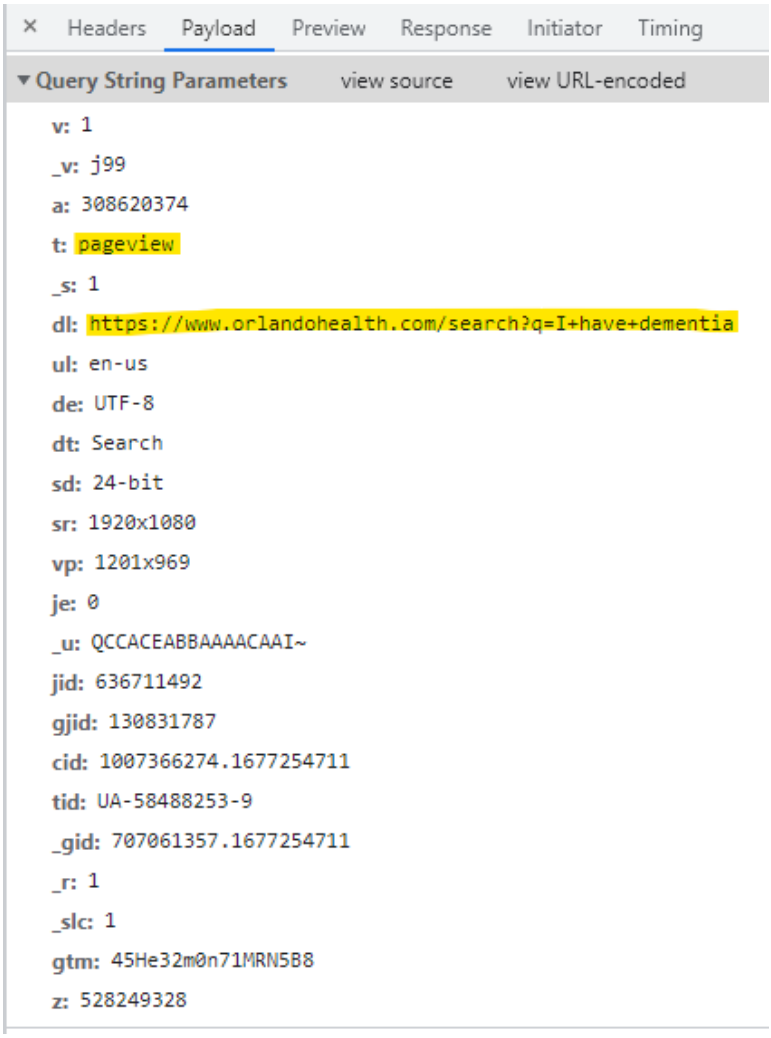
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36

93. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but other evidence suggests Defendant is using additional tracking pixels and tools to transmit its patients' Private Information to additional third parties. For example, the images below indicate that Defendant is also sending its patients' protected health information to Google via the Google Analytics tool and Google Tag Manager.

94. Both images below contain the user's search phrase ("I have dementia"), and Defendant does not appear to have enabled the anonymize feature provided by Google Analytics because the text "aip:" does not appear in either image.

▼ Request Headers

:authority: www.google-analytics.com
:method: POST
:path: /j/collect?v=1&_v=j99&a=308620374&t=pageview&_s=1&dl=https%3A%2F%2Fwww.orlandohealth.com%2Fsearch%3Fq%3DI%2Bhave%2Bdementia&ul=en-us&de=UTF-8&dt=Search&sd=24-bit&sr=1920x1080&vp=1201x969&je=0&_u=QCCACEABBAAAACAAI~&jid=636711492&gjid=130831787&cid=1007366274.1677254711&tid=UA-58488253-9&_gid=707061357.1677254711&_r=1&_slc=1&gtm=45He32m0n71MRN5B8&z=528249328
:scheme: https
accept: */*
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
content-length: 0
content-type: text/plain
origin: https://www.orlandohealth.com
referer: https://www.orlandohealth.com/
sec-ch-ua: "Not_A Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
sec-fetch-dest: empty
sec-fetch-mode: cors
sec-fetch-site: cross-site
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36



95. Accordingly, Google receives patients' communications alongside the patients' IP address, which is also impermissible under HIPAA.

96. Defendant does not disclose that the Pixel embedded in the Source Code for orlandohealth.com tracks and transmits Plaintiff's and Class Members' Private Information to Facebook.

97. In addition, upon information and belief and as described above, Defendant has also installed Conversions API on its servers to record and store the user's Website

interactions and Private Information, which is then transmitted directly to Facebook by Defendant.

98. Defendant does not disclose that the Conversions API installed on the servers for orlandohealth.com tracks, records, and transmits Plaintiff's and Class Members' Private Information to Facebook.

99. Defendant never received consent or written authorization to disclose to Facebook the Private Information entered by Plaintiff and Class Members on orlandohealth.com.

iii. Plaintiff W.W.'s Experiences

100. Plaintiff submitted medical information to Defendant via the Website. Because Defendant utilizes the Facebook Pixel, the Website's Source Code sends a secret set of instructions back to the individual's browser, causing the Pixel to send Plaintiff's FID, the Pixel ID, and the webpage's URL to Facebook.

101. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients' FIDs, IP addresses, and/or device IDs or other information they input into Defendant's Website, like their home address, zip code, or phone number. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.[26] Plaintiff's and Class Members identities could be easily

[26] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Nov. 14, 2022)

determined based on the FID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

102. 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, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity. A user's Facebook Profile ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—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.

103. In sum, Defendant's Pixel transmitted Plaintiff's highly sensitive communications and Private Information to Facebook, including communications that contained Private and confidential information, without Plaintiff's knowledge, consent, or express written authorization

104. Defendant breached Plaintiff's right to privacy and unlawfully disclosed her Private Information to Facebook. Specifically, Plaintiff had a reasonable expectation of privacy, based on her status as Defendant's patient, that Defendant would not disclose her Private Information to third parties.

105. Defendant did not inform Plaintiff that it shared her Private Information with Facebook.

106. By doing so without Plaintiff's consent, Defendant breached Plaintiff's and Class Members' right to privacy and unlawfully disclosed Plaintiff's Private Information.

107. Upon information and belief, as a "redundant" measure to ensure Plaintiff's Class Members' Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's and Class Members' Private Information from electronic storage on Defendant's server directly to Facebook.

108. Plaintiff suffered damages in the form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the invasion of privacy; (iii) diminution of value of the Private Information; (iv) statutory damages; (v) the continued and ongoing risk to her Private Information; and (vi) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiff's medical conditions and other confidential information she communicated to Defendant via the Website.

109. Plaintiff has a continuing interesting in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

C. Defendant's Conduct Is Unlawful and Violates Its Patients' Rights.

i. Defendant Violated HIPAA Standards

110. 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.[27]

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

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

> 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.[28]

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

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a

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

[28]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022).

> covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added).[29]

114. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[30]

115. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

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

ii. Defendant Violated Industry Standards

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

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

---

[29]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Nov. 3, 2022)

[30] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

119. AMA Code of Ethics Opinion 3.1.1 provides:

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

120. AMA Code of Medical Ethics Opinion 3.2.4 provides:

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

121. AMA Code of Medical Ethics Opinion 3.3.2 provides:

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

iii. Plaintiff's and Class Members' Expectation of Privacy

122. Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

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

iv. IP Addresses Are Personally Identifiable Information

124. On information and belief, through the use of the Facebook Pixel on Defendant's Website, Defendant also disclosed and otherwise assisted Facebook with intercepting Plaintiff's and Class Members' Computer IP addresses.

125. An IP address is a number that identifies the address of a device connected to the Internet.

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

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

128. Facebook tracks every IP address ever associated with a Facebook user.

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

130. Under HIPAA, an IP address is considered personally identifiable information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).
- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an

individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

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

v. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

132. The sole purpose of the use of the Facebook Pixel on Defendant's Website was marketing and profits.

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

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

135. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

D. Plaintiff's and Class Members' Private Information Had Financial Value.

136. Plaintiff's data and Private Information has economic value. Facebook regularly uses data that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences and then sells that information to advertising clients.

137. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." 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.

138. 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.[31]

139. 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."[32]

TOLLING

140. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that her PII and PHI was intercepted and unlawfully disclosed to Facebook because Defendant kept this information secret.

[31] *See* https://time.com/4588104/medical-data-industry/ (last visited February 16, 2023).

[32] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited February 16, 2023).

CLASS ACTION ALLEGATIONS

141. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

142. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent as a result of using Defendant's Website (the National Class).**

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

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

145. Numerosity, Fed R. Civ. P. 23(a)(1). The National Class members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds of thousands of individuals whose PII and PHI may have been improperly disclosed to Facebook, and the Class is identifiable within Defendant's records.

146. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

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

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

c. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

d. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

e. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

g. Whether Defendant violated the consumer protection statutes asserted as claims in this Complaint;

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

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

147. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

148. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

149. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

150. Policies Generally Applicable to the Class. Fed. R. Civ. P. 23(b)(2). This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

151. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

152. The litigation of the claims is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

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

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

154. Unless a class-wide injunction is issued, Defendant may continue disclosing the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

155. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

156. Issue Certification, Fed. R. Civ. P. 23(c)(4). Likewise, particular issues 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, the following:

a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;

b. Whether Defendant breached a legal duty to Plaintiff 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 Plaintiff 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.

157. Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

COUNT I
VIOLATION OF THE FLORIDA SECURITY COMMUNICATIONS ACT
(On Behalf of Plaintiff and the National Class)

158. Plaintiff repeats and re-alleges paragraphs 36-38, 68-99, 100-109, and 110-135 contained in the Complaint as if fully set forth herein.

159. The Florida Secretary of Communications Act ("FSCA") is codified at Florida Statutes, § 934.01, et seq. The FSCA begins with legislative findings, including:

> On the basis of its own investigations and of published studies, the Legislature makes the following findings…(4) to safeguard the privacy of innocent persons, the interception of wire or oral communications when none of the parties to the communications has consented to the interceptions should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court.

160. Florida Statutes § 934.10 provides, in pertinent part, as follows:

> Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of §§ 934.04-934.09 shall have a civil cause of action against any person or entity who intercepts, discloses, or uses, or procures any person or entity to intercept, disclose, or use, such communications and shall be entitled to recover from any such person or entity which engaged in that violation such relief as may be appropriate, including: (a) [p]reliminary or equitable declaratory relief as may be appropriate; (b) [a]ctual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of the violation or $1,0000, whichever is higher; (c) [p]unitive damages; and (d) [a] reasonable attorney's fee and other litigation costs reasonably incurred.

161. The FCSA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in party by a wire, radio, electromagnetic, photoelectronic, or photo-optical systems that affects intrastate, interstate, or foreign commerce." Fla. Stat. § 934.02(12). It further defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Fla. Stat. § 934.02(3).

162. At all relevant times, Defendant aided, employed, agreed with, and conspired with Facebook to intercept Plaintiff's and Class Members' internet communications while accessing orlandohealth.com, including the contents thereof—*i.e.*, the URL visited, the medical conditions and types of doctors searched, whether and with whom the patient had a medical televisit, payment of medical bills, and the contents of any live chats. Such information not only constitutes protected health information, but it also represents the substance, import, and meaning of the communications between Plaintiff and other Class Members had with Defendant's Website.

163. Plaintiff and other Class Members had a reasonable expectation of privacy in the electronic communications they had with Defendant's Website. Defendant had given no indication given that Plaintiff's and Class Members' Private Information would be shared with others other than that required by law or for medical care. The application of the Facebook Pixel is not required by law or necessary for medical care.

164. Nonetheless, these electronic communications were transmitted to and intercepted by a third party (*i.e.*, Facebook) during the communication and without knowledge, authorization, or consent of Plaintiff and Class Members. That is because Defendant intentionally inserted an electronic device into its website that, without the knowledge and consent of Plaintiff and Class Members, recorded and transmitted the substance of their confidential communications with Defendant to a third party.

165. Defendant willingly facilitated Facebook's interception and collection of Plaintiff's and Class Members' Private Information by embedding the Facebook Pixel on its Website.

166. Defendant used the following items as a device or apparatus to intercept wire, electronic, or oral communications made by Plaintiff and other Class Members:

a. The computer codes and programs Facebook used to track Plaintiff's and Class Members' communications while they were navigating orlandohealth.com;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' computing and mobile devices;

d. Facebook's web and ad servers;

e. The web and ad-servers from which Facebook tracked and intercepted Plaintiff's and Class Members' communications while they were using a web browser to access or navigate orlandohealth.com;

f. The computer codes and programs used by Facebook to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit Defendant's website; and

g. The plan Facebook carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser or mobile application to visit Defendant's website.

167. Defendant fails to disclose that it is using the Facebook Pixel specifically to track and automatically and simultaneously transmit communications to a third party, *i.e.*, Facebook.

168. To avoid liability under the FCSA, a defendant must show it had the consent of all parties to a communication.

169. The patient communication information that Defendant transmits while using the Facebook Pixel, such as doctor appointment booking information and names, IP addresses, and home addresses constitutes protected health information.

170. As demonstrated hereinabove, Defendant violates the FCSA by aiding and permitting third parties to receive its patients' online communications in real time through its Website without their consent.

171. By disclosing Plaintiff's and Class Members' Private Information, Defendant violated Plaintiff's and Class Members' statutorily protected privacy rights.

172. As a result of the above violations and pursuant to Florida Statutes, § 934.10, Plaintiff and Class Members are entitled to actual damages or liquidated damages of $1,000 or $100 per day for each violation, whichever is higher.

173. Under the statute, Defendant is also liable for reasonable attorneys' fees, reasonable litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

COUNT II
INVASION OF PRIVACY UNDER FLORIDA CONSTITUTION
(On Behalf of Plaintiff and the National Class)

174. Plaintiff repeats and re-alleges paragraphs 36-38, 68-99, 100-109, and 110-135 contained in the Complaint as if fully set forth herein.

175. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications, and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion, or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

176. At all relevant times, by using Facebook's Tracking Pixel to record and communicate patients' FIDs and other individually identifying information alongside their

confidential medical communications, Defendant intentionally invaded Plaintiff's and Class Members' privacy rights under the Florida Constitution.

177. Plaintiff and Class Members had a reasonable expectation that their communications, identity, health information, and other data would remain confidential and that Defendant would not install a device or apparatus on the Website to securely intercept and transmit their electronic communications to a third party.

178. Plaintiff and Class Members did not authorize Defendant to record and transmit Plaintiff's and Class Members' Private Information alongside their personally identifiable health information.

179. This invasion of privacy is serious in nature, scope, and impact because it relates to patients' Private Information. Moreover, it constitutes an egregious breach of the societal norms underlying their privacy rights.

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

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

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

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

184. Plaintiff also seek other such relief as the Court may deem just and proper.

COUNT III
INVASION OF PRIVACY
(On Behalf of Plaintiff and the National Class)

185. Plaintiff repeats and re-alleges paragraphs 36-38, 68-99, 100-109, and 110-135 contained in the Complaint as if fully set forth herein.

186. The Private Information of Plaintiff and Class Members consists of private and confidential facts and information that was never intended to be shared beyond private communications.

187. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information shared on Defendant's Website and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

188. Defendant owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

189. Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information to Facebook, a third-party social media and marketing giant, is highly offensive to a reasonable person.

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

191. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiff's and Class Members' privacy because Defendant facilitated Facebook's simultaneous eavesdropping and wiretapping of confidential communications.

192. Defendant failed to protect Plaintiff's and Class Members' Private Information and acted knowingly when it installed the Pixel onto its Website because the purpose of the Pixel is to track and disseminate individual's communications with the Website for the purpose of marketing and advertising.

193. Because Defendant intentionally and willfully incorporated the Facebook Pixel into its Website and encouraged patients to use that Website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff and Class Members.

194. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiff and the Class Members was disclosed to a third party without authorization, causing Plaintiff and the Class to suffer damages.

195. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy

interest invaded by Defendant, loss of time and opportunity costs, plus prejudgment interest, and costs.

196. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant and is still in the possession of Facebook and the wrongful disclosure of the information cannot be undone.

197. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook who on information and belief continues to possess and utilize that information.

198. Plaintiff, on behalf of herself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the National Class)

199. Plaintiff repeats and re-alleges paragraphs 36-38, 68-99, 100-109, and 110-135 contained in the Complaint as if fully set forth herein.

200. As a condition of utilizing Defendant's digital platforms and receiving services from Defendant, Plaintiffs and the Class provided their Private Information and compensation for their medical care.

201. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

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

203. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information without consent to third parties like Facebook.

204. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of Private Information.

205. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiff and the National Class)

206. Plaintiff repeats and re-alleges paragraphs 36-38, 68-99, 100-109, 110-135, and 136-139 contained in the Complaint as if fully set forth herein.

207. Defendant benefits from the use of Plaintiff's and Class Members' Private Information and unjustly retained those benefits at their expense.

208. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation. Defendant consciously and voluntarily collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

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

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

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

COUNT VI
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(1) *et seq*.
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of Plaintiff and the National Class)

212. Plaintiff repeats and re-alleges paragraphs 36-38, 68-99, 100-109, and 110-135 contained in the Complaint as if fully set forth herein.

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

214. 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.

215. The transmissions of Plaintiff's Private Information to Defendant via Defendant' Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

216. The transmissions of Plaintiff's Private Information to medical professionals qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(2).

217. **Electronic Communications**. The transmission of Private Information between Plaintiff and Class Members and Defendant via its 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).

218. **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).

219. **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).

220. **Electronic, 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. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendant's web-servers; and

d. The Pixel deployed by Defendant to effectuate the sending and acquisition of patient communications

221. By utilizing and embedding the Pixel on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

222. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Private Information to Facebook.

223. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiff's and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

224. By intentionally disclosing or endeavoring to disclose the electronic communications of the Plaintiff 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).

225. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff 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).

226. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

227. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel and Conversions API to track and utilize Plaintiff's and Class Members' Private Information for financial gain.

228. Defendant was not acting under color of law to intercept Plaintiff and the Class Member's wire or electronic communication.

229. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the Pixel tracking code.

230. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

231. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious and designed to violate federal and state legal provisions, including as described above the following: (1) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (2) violation of Minn. Stat. § 325D.44, subd. 1.

COUNT VII
VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE
18 U.S.C. § 2511(3)(a)
(On Behalf of Plaintiff and the National Class)

232. Plaintiff repeats and re-alleges paragraphs 36-38, 68-99, 100-109, and 110-135 contained in the Complaint as if fully set forth herein.

233. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

234. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

235. Defendant's Website is an electronic communication service that gives users the ability to send or receive electronic communications to Defendant and, upon information and belief, medical professionals who contract with, but are not employed by Defendant. In the absence of Defendant's Website, internet users could not send or receive communications regarding Plaintiff's and Class Members' Private Information.

236. Defendant's Website is a conduit of communication between Plaintiff and Class Members and their respective medical providers, including third parties who are not employed by Defendant, but contract with Defendant to provide medical treatment and services for its patients.

237. **Intentional Divulgence**. Defendant intentionally designed and/or implemented the Pixel and Conversions API tracking and was or should have been aware that it could divulge Plaintiff's and Class Members' Private Information.

238. **While in Transmission**. Upon information and belief, Defendant's divulgence of the contents of Plaintiff's and Class Members' communications was contemporaneous with their exchange with Defendant's Website, to which they directed their communications.

239. Defendant divulged the contents of Plaintiff's and Class Members' electronic communications without authorization. Defendant divulged the contents of Plaintiff's and Class Members' communications to Facebook without Plaintiff's and Class Members' consent and/or authorization.

240. **Exceptions do not apply**. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication":

- "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"
- "with the lawful consent of the originator or any addressee or intended recipient of such communication;"
- "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or
- "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

U.S.C. § 2511(3)(b).

241. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

242. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on Defendant's Website to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant's service; nor (2) necessary to the protection of the rights or property of Defendant.

243. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

244. Defendant's divulgence of the contents of user communications on Defendant's browser through the Pixel and Conversions API code was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Websites or apps with which Plaintiff and Class Members were exchanging information.

245. Moreover, Defendant divulged the contents of Plaintiff and Class Members' communications through the Facebook Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

246. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

247. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; and reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT VIII
VIOLATION OF TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 18 U.S.C. § 2702, *et seq.* (STORED COMMUNICATIONS ACT) (On Behalf of Plaintiff and the National Class)

248. Plaintiff repeats and re-alleges paragraphs 36-38, 68-99, 100-109, and 110-135 contained in the Complaint as if fully set forth herein.

249. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

250. **Electronic Communication Service.** ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

251. Defendant's Website is a conduit of communication between Plaintiff and Class Members and their respective medical providers, including third parties who are not employed by Defendant, but contract with Defendant to provide medical treatment and services for its patients.

252. Defendant's Website is also a conduit between Plaintiff and Class Members and Defendant.

253. Defendant intentionally procures and embeds various Plaintiff's Private Information through the Pixel and Conversions API used on Defendant's Website, which qualifies as an Electronic Communication Service.

254. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

255. Defendant stores the content of Plaintiff's and Class Members' communications with Defendant's Website and files associated with it via the Pixel or Conversions API. As explained above, via Conversions API, Defendant stores Plaintiff's

and Class Members' Private Information on its servers and then transmits that Private Information to Facebook.

256. By way of another example, Defendant stores data pertaining to scheduling appointments, IP addresses, and communications regarding medical treatment.

257. When Plaintiff or Class Member communicates with the Website, the content of that communication is immediately placed into storage.

258. Defendant knowingly divulges the contents of Plaintiff's and Class Members' communications through its Website's source code.

259. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication—"

a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."

b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;"

c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"

d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"

e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;"

f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A."

g. "to law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;"

h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or

i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

260. Defendant did not divulge the contents of Plaintiff's and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiff and Class Members.

261. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

262. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

263. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on Defendant's Website to Facebook was not authorized by 18 U.S.C. §

2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

264. Defendant's divulgence of the contents of user communications on Defendant's Website was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Websites or apps with which Plaintiff and Class Members were exchanging information.

265. Moreover, Defendant divulged the contents of Plaintiff's and Class Members' communications through the Facebook Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

266. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

267. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages if applicable in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT IX
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (CFAA)
18 U.S.C. § 1030, *et seq*.
(On Behalf of Plaintiff and the National Class)

268. Plaintiff repeats and re-alleges paragraphs 36-38, 68-99, 100-109, and 110-135 contained in the Complaint as if fully set forth herein.

269. The Plaintiff's and the Class Members' computers and/or mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

270. Defendant exceeded, and continues to exceed, authorized access to the Plaintiff's and the Class Members' protected computers and obtained information thereby, in violation of 18 U.S.C. §§ 1030(a)(2), 1030(a)(2)(C).

271. For example, Defendant exceeded its unauthorized access because Defendant accessed Plaintiff's and Class Members' Private Information under false pretenses, *i.e.*, Defendant did not disclose it was transmitting Private Information to Facebook.

272. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiff's and the Class Members' private and personally identifiable data and content – including the Website visitor's electronic communications with the Website, URLs of web pages visited, and/or other electronic communications in real-time which were never intended for public consumption.

273. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV) due to the Private Information of Plaintiff and the

Class being made available to Defendant, Facebook, and/or other third parties without adequate legal privacy protections.

274. Accordingly, Plaintiff and the Class are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

COUNT X
BREACH OF CONFIDENCE
(On behalf of Plaintiff and the National Class)

275. Plaintiff repeats and re-alleges paragraphs 36-38, 68-99, 100-109, and 110-135 contained in the Complaint as if fully set forth herein.

276. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

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

278. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Pixel and Conversions API to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant, including Private Information and the contents of such information.

279. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

280. The third-party recipients included, but may not be limited to, Facebook. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

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

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

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

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

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

e. Nominal damages for each independent violation;

f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;

g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and

i. Defendant's actions violated the property rights Plaintiff and Class members have in their Private Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the National Class and appointing Plaintiff and Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

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

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

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demand that this matter be tried before a jury.

DATE: March 16, 2023

Respectfully Submitted,

/s/ Jonathan B. Cohen
Jonathan B. Cohen (FL Bar No. 27620)
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
3833 Central Ave.
St. Petersburg, FL 33713
Phone: (813) 786-8622
Email: jcohen@milberg.com

Bryan L. Bleichner* (MN BAR #0326689)
Jeffrey D. Bores* (MN BAR #0227699)
Philip J. Krzeski* (MN BAR #0403291)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
jbores@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Gary M. Klinger*
Glen L. Abramson*
Alexandra M. Honeycutt*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com
gabramson@milberg.com
ahoneycutt@milberg.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court St., Ste. 530
Cincinnati, Ohio 4502
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Joseph M. Lyon*
The Lyon Law Firm
2754 Erie Ave.
Cincinnati, Ohio 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Counsel for Plaintiff and the Putative Class

* *pro hac vice* forthcoming