SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF KINGS

ERYN KAPLAN, MICHAEL ZURL and KATHYANN MCCLENDON, *on behalf of themselves and all others similarly situated*, Plaintiffs, v. NORTHWELL HEALTH, Defendant.	Index No. **COMPLAINT** **JURY TRIAL DEMANDED**

TO THE SUPREME COURT OF NEW YORK:

Plaintiffs Eryn Kaplan, Michael Zurl, and Kathyann McClendon, by their attorneys, as and for their Complaint against Defendant, state as follows:

NATURE OF THE ACTION

1. Plaintiffs Eryn Kaplan, Michael Zurl, and Kathyann McClendon ("Plaintiffs"), at all times relevant herein, have been patients at Northwell Health, Inc. ("Northwell" or "Defendant"), and bring this class action individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions, their counsels' investigation, and upon information and belief as to all other matters, as follows:

2. Plaintiffs bring this case to address Defendant's unlawful practice of disclosing its patients' confidential information, including personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information"), to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook") and Google, Inc. ("Google") without consent, through the use of tracking software that is embedded in Defendant's website.

3. Defendant owns and controls https://www.northwell.edu ("Defendant's Website" or the "Website"), which it encourages patients to use for finding and booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions, treatment options, and more.

4. Unbeknownst to Plaintiffs and Class Members, however, Defendant embedded tracking technologies onto its Website including, for example, the Facebook Pixel and Google Analytics (the "Tracking Tools"), which surreptitiously forced Plaintiffs and Class Members to transmit their Private Information to Facebook, Google, and other third parties.

5. Through the Website, Defendant advertises to its prospective and current patients that its online functionality is a secure and private means of interacting with Defendant and its healthcare providers.

6. However, operating as designed and as implemented by Defendant, the Tracking Tools allow the Private Information that Plaintiffs and Class Members submit to Defendant to be unlawfully disclosed to third parties alongside personally identifiable information such as the individual's unique and persistent Facebook ID ("FID")[1], IP addresses, and the like.

7. The Tracking Tools consist of computer code that transmits a patient's communications with a website to a third party. Included in these communications are the text or phrases the website visitor types into various portions of the website (such as a general search bar, chat feature, or text box), descriptive URLs that show the information being communicated, and buttons clicked in response to queries from the website, among other things.

[1] 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/.

8. The patient's web browser executes the Tracking Tools via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Tracking Tools are customizable and programmable, meaning that the website owner controls which of its webpages contain the Tracking Tools, which events are tracked and transmitted to third parties like Facebook and Google, and what information from the communications are disclosed.

9. When a patient visits a webpage containing the Tracking Tools, their device is commandeered, and their communications are surreptitiously duplicated and transmitted to third parties.

10. The information sent to third parties included the Private Information that Plaintiff sand Class Members submitted to Defendant's Website related to their past, present, or future health conditions, including, for example, the type and date of a medical appointment. Such Private Information would allow the third party (e.g., Facebook or Google) to know that a specific patient was seeking confidential medical care from Defendant as well as the type of medical care being sought. This disclosure would also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, or addiction.

11. Simply put, by installing the Tracking Tools into its Website, Defendant effectively planted a bug on Plaintiffs' and Class Members' web browsers and compelled their browsers to disclose their communications with Defendant to unauthorized third parties.

12. In addition to the Tracking Tools, upon information and belief Defendant also installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on its Website servers.[2]

13. 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.[3, 4] 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."[5]

14. 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.

15. 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 specific customers by utilizing data and information from users' communications with the Website to build profiles for

[2] "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/.
[3] https://revealbot.com/blog/facebook-conversions-api/.
[4] "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.
[5] https://www.facebook.com/business/help/204114870265296?id=818859032317965.

the purposes of retargeting and future marketing. Facebook also uses Plaintiffs' and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

16. The information disclosed in this way by Defendant allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who geotarget Plaintiffs' and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and CAPI.

17. 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 or Google, which both have a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patients' consent.

18. Neither Plaintiffs nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook, Google, or any other third party, nor did they provide affirmative express consent.

19. Despite willfully and intentionally incorporating the Tracking Tools and CAPI into its Website and servers, Defendant has never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook, Google, or other third parties. Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously transmitted to third parties 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.

20. Defendant breached its statutory and common law obligations to Plaintiffs and Class Members by, *inter alia*, (i) failing to remove or disengage technology that was known and designed to share web-users' information; (ii) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook, Google, or others; (iii) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through tracking technologies like the Facebook Pixel, Google Analytics, and CAPI; (iv) failing to warn Plaintiffs and Class Members; and (v) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

21. As a result of Defendant's conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of the bargain, (iii) diminution of value of the Private Information, (iv) statutory damages, and (v) the continued and ongoing risk to their Private Information.

22. Plaintiffs seek to remedy these harms and bring causes of action for (1) breach of fiduciary duty/confidentiality; (2) violation of the Electronics Communication Privacy Act ("ECPA") 18 U.S.C. § 2511(1) – unauthorized interception, use, and disclosure; (3) invasion of privacy; (4) breach of implied contract; (5) unjust enrichment; (6) negligence; and (7) violation of the New York Consumer Law for Deceptive Acts and Practices Gen. Bus. Law § 349.

PARTIES

23. Plaintiff Eryn Kaplan is a natural person and citizen of New York where she intends to remain.

24. Plaintiff Michael Zurl is a natural person and citizen of New York where he intends to remain.

25. Plaintiff Kathyann McClendon is a natural person and citizen of New York where she intends to remain.

26. Defendant Northwell is a health care provider incorporated as a municipal healthcare network in the State of New York and headquartered at 2000 Marcus Ave, New Hyde Park, New York 11042.

27. Defendant Northwell Health is a not-for-profit healthcare organization that provides comprehensive health care to New Yorkers through a network of hospitals, community-based health centers, long-term care and rehabilitation facilities, and specialty care services.[6] Defendant Northwell is a health network with more than 900 patient care locations spanning across the five boroughs and Long Island.[7] In addition, Northwell has more than 85,000 health care professionals and treats over 2 million patients a year.[8]

28. 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

29. This Court has subject matter jurisdiction pursuant to NY Constitution Article VI, § 7(a), which grants the Supreme Court general original jurisdiction in law and equity. The amount in controversy exceeds the jurisdictional limits of all lower courts.

30. This Court has personal jurisdiction over Defendant because it is a domestic corporation incorporated under New York law with several locations in Kings County, New York.

[6] https://www.northwell.edu/about-northwell.
[7] *Id.*
[8] *Id.*

31. Venue is proper in Kings County pursuant to CPLR § 503(a) and (c) because Defendant maintains locations in Kings County and a substantial part of the events or omissions giving rise to the claims occurred in Kings County.

COMMON FACTUAL ALLEGATIONS

A. The U.S. Department of Health and Human Services and Federal Trade Commission Have Warned about Use of Tracking Tools by Healthcare Providers

32. HHS has warned healthcare providers that Protected Information is not limited exclusively to patient portals like MyChart, and thus Defendant still has an obligation to protect information on non-password protected (i.e., "unauthenticated") webpages:

> Tracking technologies on a regulated entity's unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances. ***For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.***[9]

33. In addition, HHS and the FTC have recently issued a letter, once again admonishing entities like Defendant to stop using Tracking Tools:

> If you are a covered entity or business associate ("regulated entities") under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium. ***The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (e.g., tracking technology vendors) includes PHI. . .*** Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. . . As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information

[9] *Id*. (emphasis added)

> to third parties via technologies you have integrated into your website or app. The disclosure of such information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule.[10]

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

34. Defendant purposely installed the Tracking Tools on many of its webpages within its Website and programmed those webpages to surreptitiously share its patients' private and protected communications with Facebook, Google, and others, including communications that contain Plaintiffs' and Class Members' PHI and PII.

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

36. In order to understand Defendant's unlawful data-sharing practices, it is important first to understand basic web design and tracking tools.

C. Facebook's Business Tools and the Pixel.

37. Facebook is the largest social networking site on the planet, touting 2.9 billion monthly active users.[11] Facebook describes itself as a "real identity platform,"[12] meaning users are allowed only one account and must share "the name they go by in everyday life."[13] To that end,

---

[10] *Re: Use of Online Tracking Technologies*, U.S. Dept. of Health & Hum. Servs. and Fed. Trade. Comm'n (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf.
[11] Sean Burch, *Facebook Climbs to 2.9 Billion Users, Report 29.1 Billion in Q2 Sales* (July 28, 2021), https://www.yahoo.com/now/facebook-climbs-2-9-billion-202044267.html.
[12] Sam Schechner and Jeff Horwitz, How Many Users Does Facebook Have? The Company Struggles to Figure It Out, WALL. ST. J. (Oct. 21, 2021).
[13] COMMUNITY STANDARDS, PART IV: INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

when creating an account, users must provide their first and last name, along with their birthday and gender.[14]

38. 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.[15]

39. 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.

40. 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 communications and activity on those platforms.

41. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[16] Advertisers, such as Defendant, can track other user actions and communications and can create their own tracking parameters by building a "custom event."[17]

---

[14] SIGN UP, https://www.facebook.com/.

[15] 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.

[16] SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.; *see* 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; APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[17] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

42. One such Business Tool is the Pixel which "tracks the people and type of actions they take."[18] When a user accesses a webpage that is hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers—traveling from the user's browser to Facebook's server.

43. Notably, this transmission only occurs on webpages that contain the Pixel. Thus, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook via the Pixel but for Defendant's decisions to install the Pixel on its Website.

44. Similarly, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook via Conversions API but for Defendant's decision to install and implement that tool.

45. By installing and implementing both tools, Defendant caused Plaintiffs' and Class Members' communications to be intercepted by and/or disclosed to Facebook.

46. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via certain webpages.

D. Defendant's method of transmitting Plaintiffs' and Class Members' Private Information via the Tracking Tools.

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

[18] RETARGETING, https://www.facebook.com/business/goals/retargeting.

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

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

- **Universal Resource Locator ("URL"):** a web address
- **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, GET Requests can also send data to the host server embedded inside the URL and can include cookies.
- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.[19]

50. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as "Find a Doctor" page). The HTTP Response sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the 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 implementation of the Tracking Tools is source code that does just that. The Tracking Tools act much like a traditional wiretap. When patients visit Defendant's Website via an HTTP Request to Northwell's server, the server sends an HTTP Response including the Markup that displays the webpage visible to the user and Source Code including the Tracking Tools.

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

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

55. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that savvy users cannot evade. Facebook's workaround, for example, is CAPI. CAPI is an effective workaround because it

transmits information from Defendant's own servers and does not rely on the user's web browsers. CAPI "is designed to create a direct connection between [Website hosts'] marketing data and [Facebook]."

56. Thus, the communications between patients and Defendant, which are necessary to use Defendant's Website, are actually received by Defendant and stored on its server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

57. While there is no way to confirm with certainty that a Website host like Defendant has implemented workarounds like CAPI without access to the host server, companies like Facebook instruct 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, it is reasonable to infer that Facebook's customers who implement the Facebook Pixel in accordance with Facebook's documentation will also implement the CAPI workaround.

58. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive Website content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for 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 the user's computing device, causing the device to contemporaneously and invisibly re-direct the user's communications to third parties.

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

60. In this case, Defendant employed the Tracking Tools and CAPI to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to Facebook.

61. For example, when a patient visits https://www.northwell.edu/ and selects the "Find a Doctor" button, the patient's browser automatically sends an HTTP Request to Defendant's web server. Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage. As depicted below, the user only sees the Markup, not Defendant's Source Code or underlying HTTP Requests and Responses.

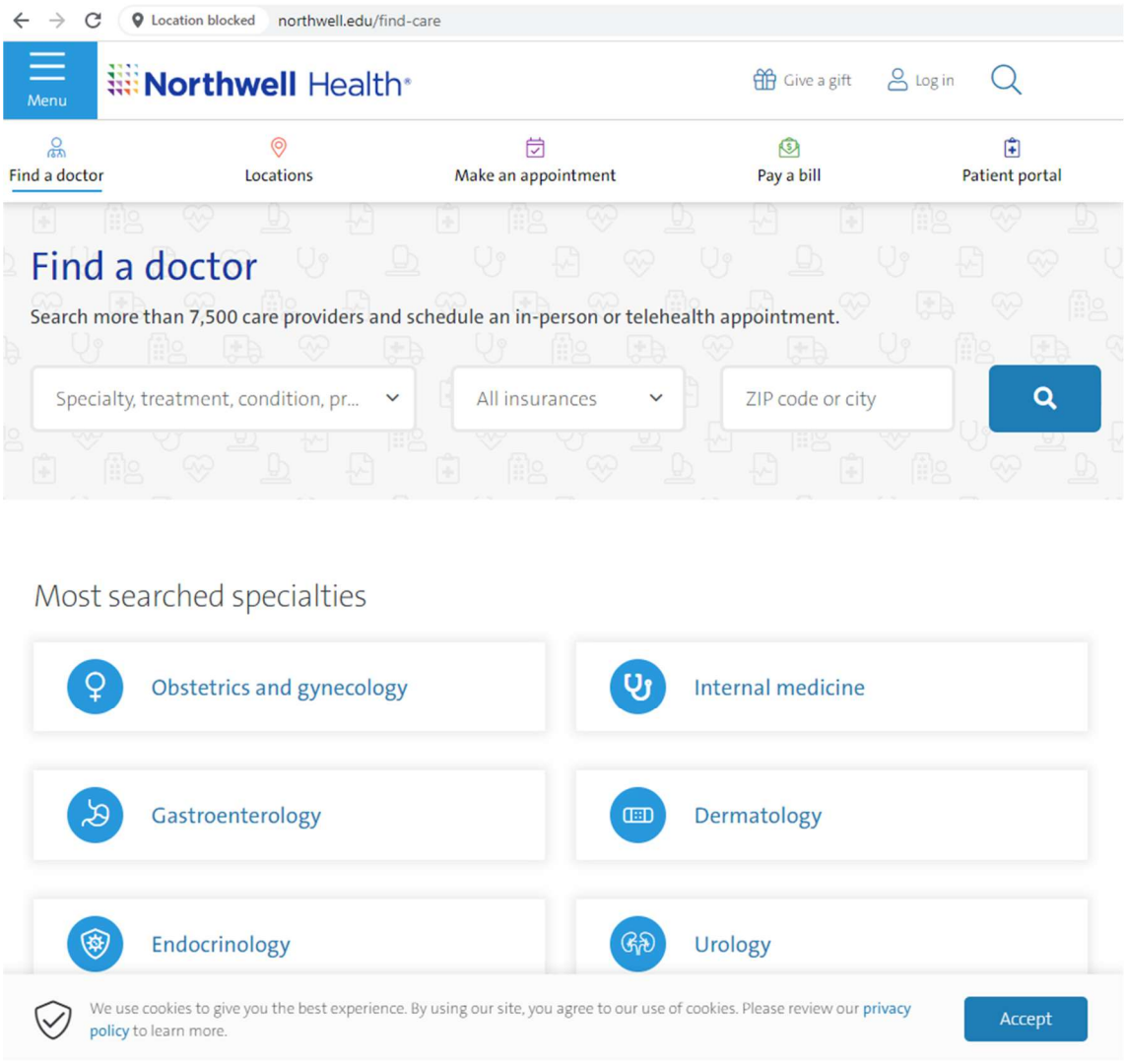


Figure 1. The image above is a screenshot taken from the user's web browser upon visiting https://www.northwell.edu/find-care *(last accessed June 9, 2023).*

62. The Facebook Tracking Pixel is one of the Tracking Tools 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]

63. Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications with Defendant and to send those communications to Facebook.

64. These transmissions occur contemporaneously, invisibly, and without the patient's knowledge.

65. Consequently, when Plaintiffs and Class Members visit Defendant's Website and communicate their Private Information, that information is intercepted by Facebook, including, but not limited to, certain phrases typed into the search box (ex. "diabetes"), names of physicians, and when a user clicks hyperlinks such as phone numbers to call physicians or hospitals.

E. Defendant Disclosed Plaintiffs' and Class Members' Private Information to Facebook Using the Pixel and/or CAPI Tracking Practices.

66. Defendant utilizes Facebook's Business Tools and intentionally installed tracking technologies like the Pixel and CAPI on its Website and servers to secretly track patients by

[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.

disclosing their communications in violation of its common law, contractual, statutory, and regulatory duties and obligations.

67. Defendant's Pixel has its own unique identifier (represented as id= 1649710231983671), which can be used to identify which of Defendant's webpages contain the Pixel.

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

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

70. Plaintiffs 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.

71. Plaintiffs and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to Facebook, nor did they intend for Facebook to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

72. The tracking technologies utilized by Defendant sent non-public Private Information to Facebook, including but not limited to Plaintiffs' and Class Members': (1) status as medical patients; (2) which physicians they sought treatment from; (3) the specialty of that physician; and (4) the location of the treatment.

73. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside the Plaintiffs' 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.[22]

74. 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 location, 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.

75. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented technology that surreptitiously tracked, recorded, and disclosed Plaintiffs' 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 Plaintiffs or Class Members and without obtaining their express written consent.

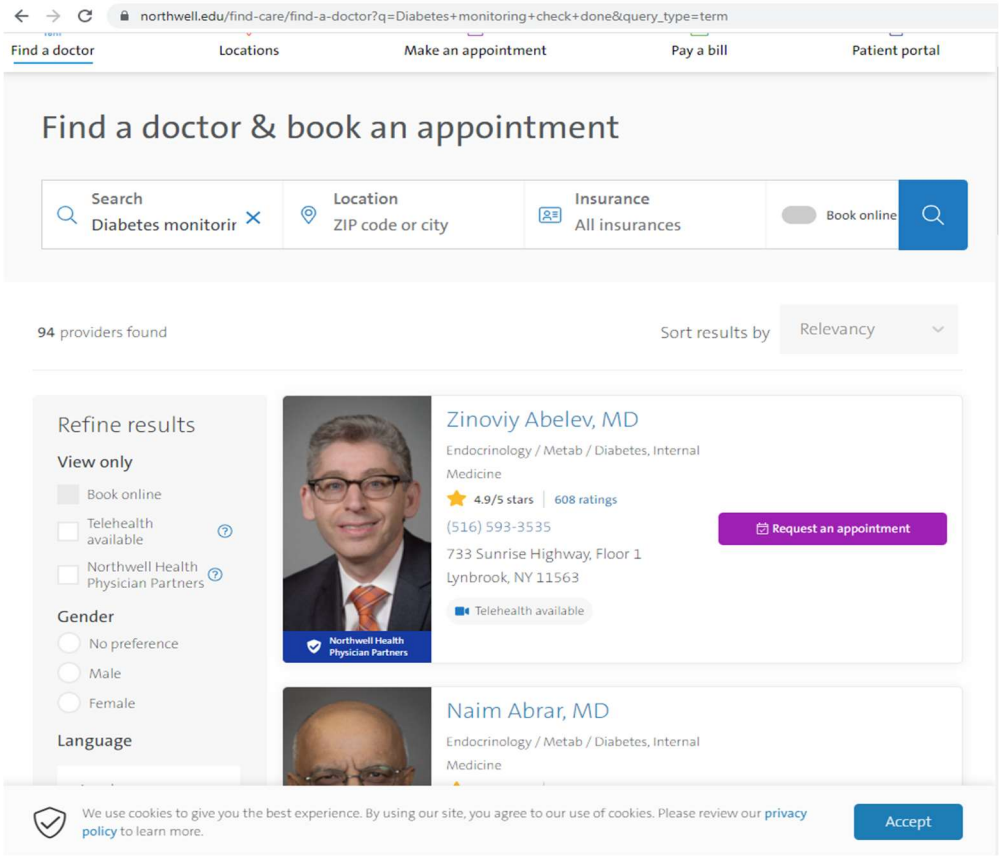
76. By installing and implementing both Facebook tools and Google Analytics, Defendant caused Plaintiffs' and Class Member's communications to be intercepted by and/or disclosed to Facebook and Google and for those communications to be personally identifiable.

[22] Defendant's Website tracks and transmits 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.

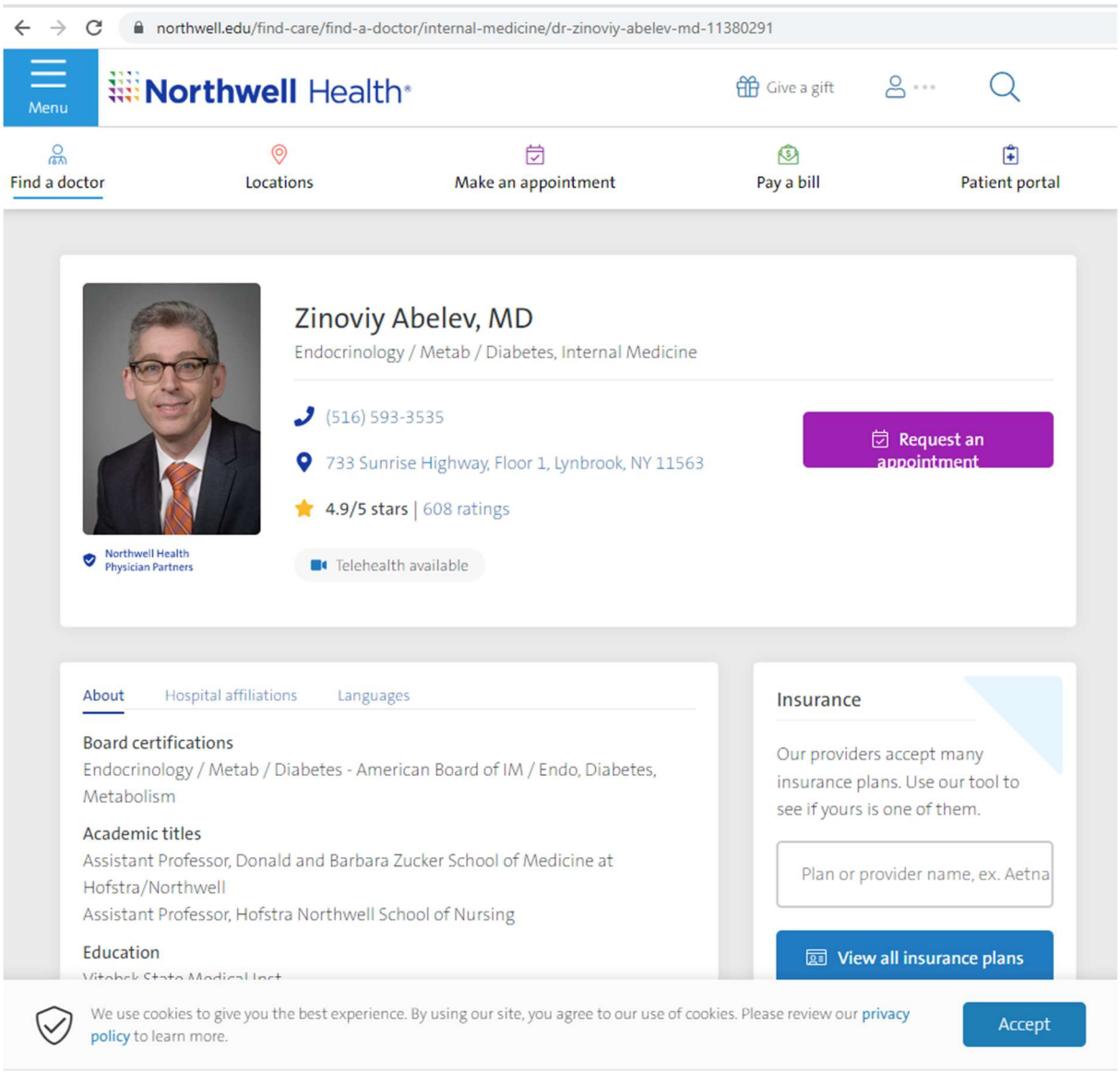
F. Defendant's Tracking Tools Force the Dissemination of Patient Information.

77. An example illustrates the point.[23] If a patient uses the Website to find a Doctor, Defendant's Website directs them to communicate Private Information, including the particular specialty the patient is seeking and the patient's zip code. Unbeknownst to the patient, each and every communication is sent to third parties via Defendant's Tracking Tools, including the physician the patient selects, the location of that physician, the patient's attempt to call that physician for an appointment, and any text or phrases the patient types into the search bar.

78. In the example below, the user navigated to the "Find a Doctor & Book an Appointment" page on Defendant's Website:



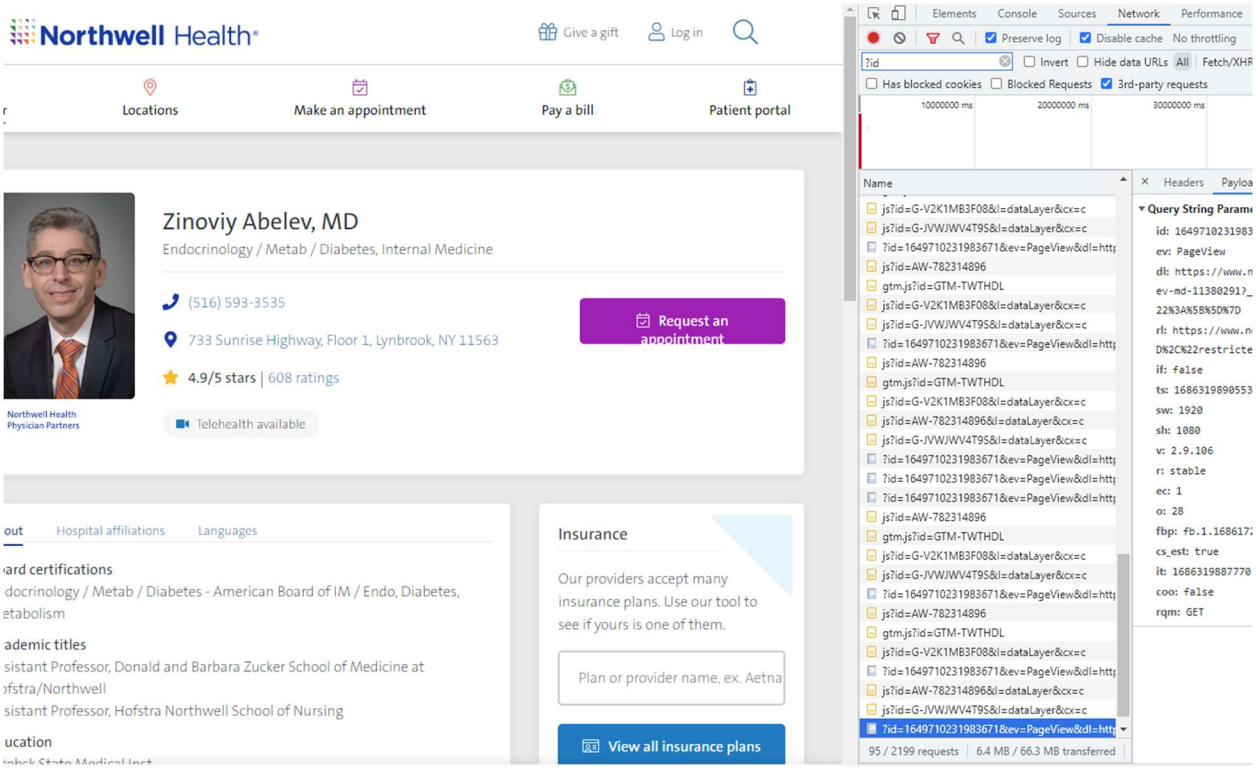
[23] The screenshots and information identified below are based on an examination of Defendant's Website from June to August of 2023. Upon information and belief, Defendant's Website may have been configured to provide even more Private Information to third parties in the past.



79. When a patient searches for "Diabetes Monitoring," which is relevant to their treatment of a specific health condition by Defendant, physicians who treat or specialize in that condition populate on the patient's screen. Next, the patient selects their physician from the list.

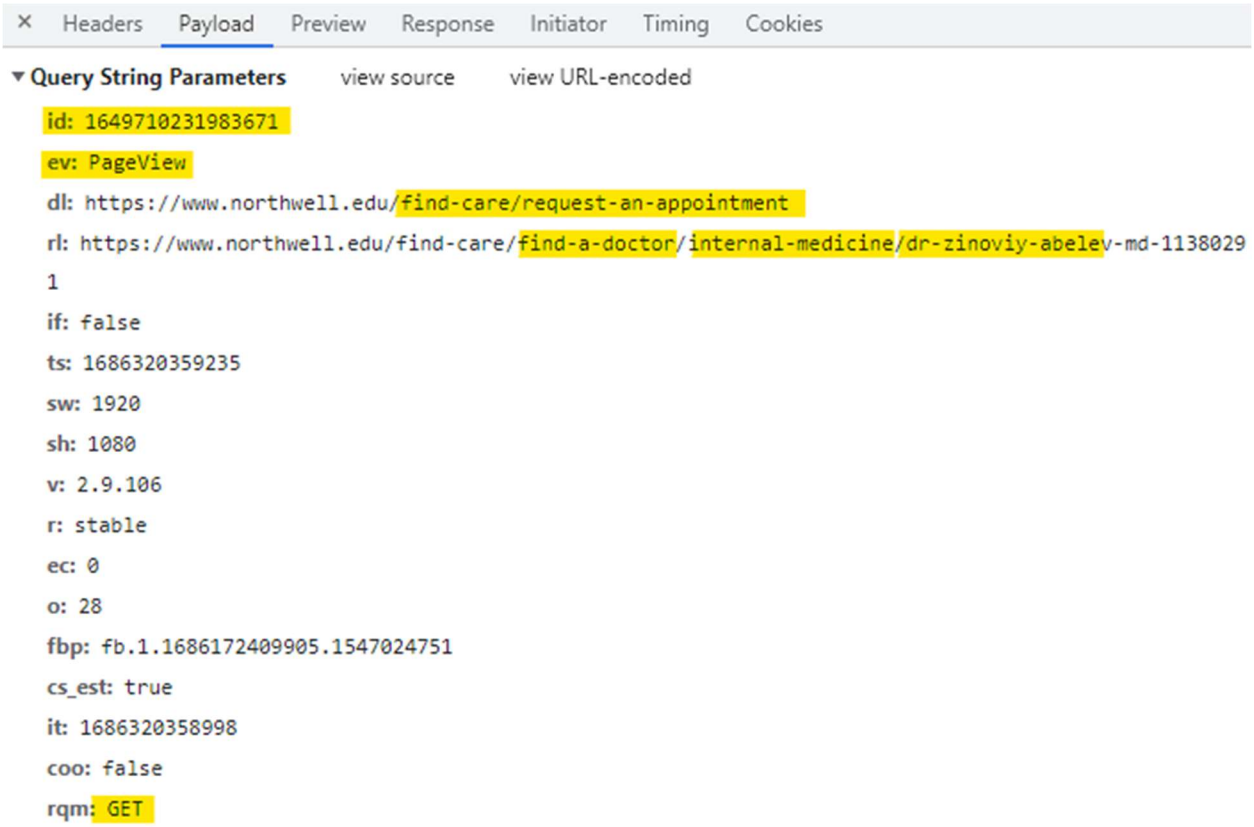
80. Unbeknownst to ordinary patients, this particular webpage— which is undoubtedly used to communicate Private Information for the purpose of seeking medical treatment —contains Defendant's Tracking Tools. The image below is a screenshot that shows the "behind the scenes" portion of the Website in the right column, which is commonly referred to as "network activity"

and invisible to ordinary users. Importantly, each entry in the right column represents just one instance in which Defendant allowed Tracking Tools to transmit the patient's Private Information to Facebook:



81. Each and every communication the patient made via the webpage was sent to Facebook, and the images below confirm that the substance of those communications—i.e. the specific health information—was received by Facebook. Importantly, the Private Information is transmitted to Facebook even if the patient has disabled third-party tracking cookies or lacks a Facebook account because a second data transmission occurs via server-to-server communications that are invisible to sophisticated users, and which does not rely on cookies.

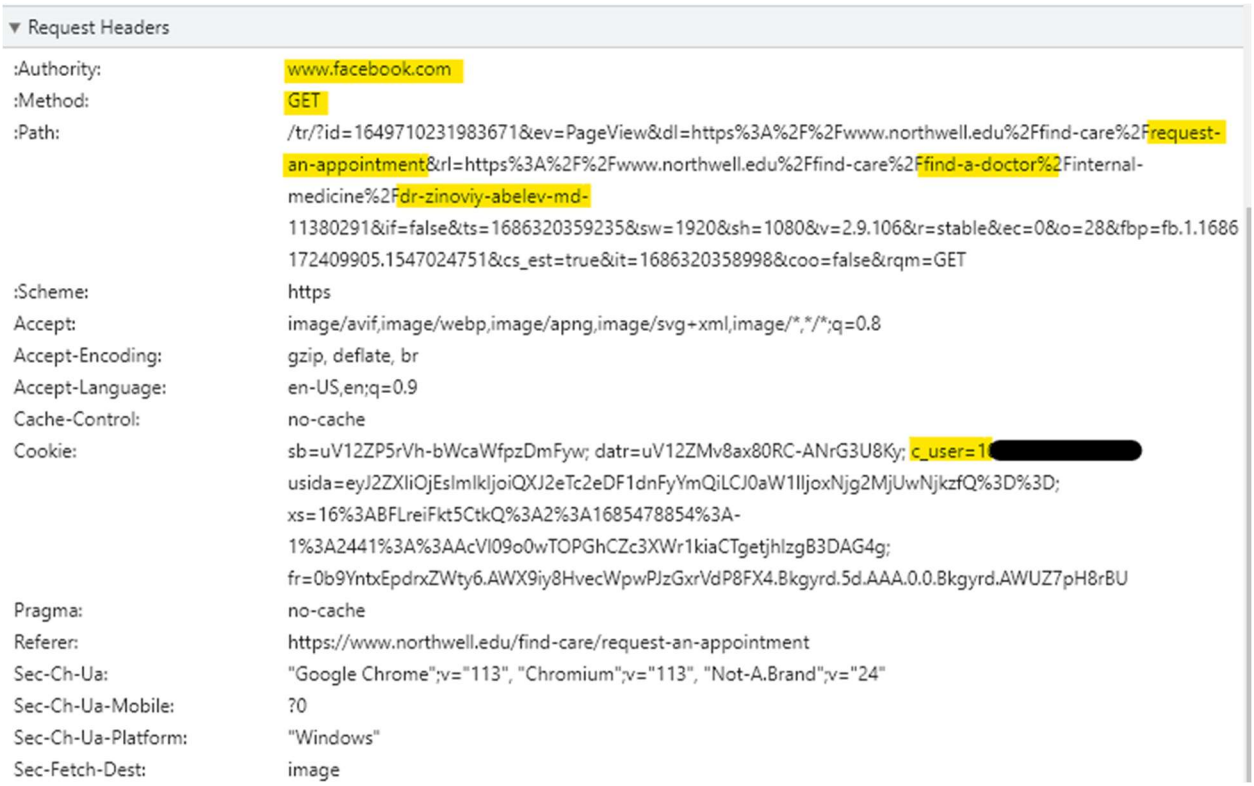
82. When Plaintiffs and other patients made online appointments, Facebook received that information alongside the selected physician's name and specialty.



83. The first line of highlighted text, "id: 1649710231983671" refers to Defendant's Pixel ID and confirms that the Defendant has downloaded Facebook's Pixel into its Source Code for this particular webpage and programmed it to disseminate patient communications—and the inherent substance of those communications—in real time.

84. The additional lines of highlighted text demonstrate that Facebook received information that allows it to identify a particular individual as a patient of Defendant, learn that the individual is seeking medical care from Defendant via www.northwell.edu, learn the name of the patient's physician, and learn the physician's specialty.

85. The highlighted text, "GET" denotes that Facebook received this communication and the Private Information contained therein, alongside the patient's Facebook ID (c_user ID), thereby linking it to their specific Facebook profile and real identity.



▼ Request Headers

:Authority:	www.facebook.com
:Method:	GET
:Path:	/tr/?id=1649710231983671&ev=PageView&dl=https%3A%2F%2Fwww.northwell.edu%2Ffind-care%2Frequest-an-appointment&rl=https%3A%2F%2Fwww.northwell.edu%2Ffind-care%2Ffind-a-doctor%2Finternal-medicine%2Fdr-zinoviy-abelev-md-11380291&if=false&ts=1686320359235&sw=1920&sh=1080&v=2.9.106&r=stable&ec=0&o=28&fbp=fb.1.1686172409905.1547024751&cs_est=true&it=1686320358998&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
Cache-Control:	no-cache
Cookie:	sb=uV12ZP5rVh-bWcaWfpzDmFyw; datr=uV12ZMv8ax80RC-ANrG3U8Ky; c_user=1[redacted] usida=eyJ2ZXIiOjEsImlkIjoiQXJ2eTc2eDF1dnFyYmQiLCJ0aW1lIjoxNjg2MjUwNjkzfQ%3D%3D; xs=16%3ABFLreiFkt5CtkQ%3A2%3A1685478854%3A-1%3A2441%3A%3AAcVl09o0wTOPGhCZc3XWr1kiaCTgetjhlzgB3DAG4g; fr=0b9YntxEpdrxZWty6.AWX9iy8HvecWpwPJzGxrVdP8FX4.Bkgyrd.5d.AAA.0.0.Bkgyrd.AWUZ7pH8rBU
Pragma:	no-cache
Referer:	https://www.northwell.edu/find-care/request-an-appointment
Sec-Ch-Ua:	"Google Chrome";v="113", "Chromium";v="113", "Not-A.Brand";v="24"
Sec-Ch-Ua-Mobile:	?0
Sec-Ch-Ua-Platform:	"Windows"
Sec-Fetch-Dest:	image

86. The image above demonstrates that the user's Facebook ID (highlighted as "c_user=" in the image) was sent alongside the contents of the communication. [24]

87. Thus, Plaintiffs' and other patients' website activity was received by Facebook alongside their personally identifiable information.

88. Marketers and data brokers can use a variety of methods to identify individual website users, and HHS has expressly stated that individual strings of numbers, innocuous as they may seem, are personally identifiably information, with IP addresses being the most cited example.

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

The c_user cookie containing a patient's Facebook ID is just one example of a persistent identifier, but Facebook also received patients' IP addresses and other device IDs.[25]

89. The c_user cookie containing patients' Facebook IDs is commonly referred to as a third-party cookie because it was "created by a website with a domain name other than the one the user is currently visiting"—*i.e.*, Facebook.

90. Although Facebook created the cookie, Defendant is ultimately responsible for the manner in which individual patients were identified because it is in complete control of how the Pixel was implemented on its website. Stated differently, Facebook would not have received *any* patient communications made via northwell.edu and related web properties but-for Defendant's implementation and use of the Pixel.

91. Additionally, Facebook and other third parties would not receive the contents of patient communications—such as specific treatments, medical diagnosis, symptoms, and physicians' names—if Defendant properly coded its website. Had that been the case, and it is not, the Pixel would have merely revealed that the Plaintiffs visited the website. Instead, Facebook received specific details pertaining to their medical conditions and treatment.

92. In addition to third-party cookies, Defendant also revealed its patients' identities via first-party cookies, such as the _fbp cookie, and a recent browsing session captured in the image below demonstrates the Defendant is currently using over a dozen first-party cookies that transmit patient information for marketing purposes and monetize patient data:

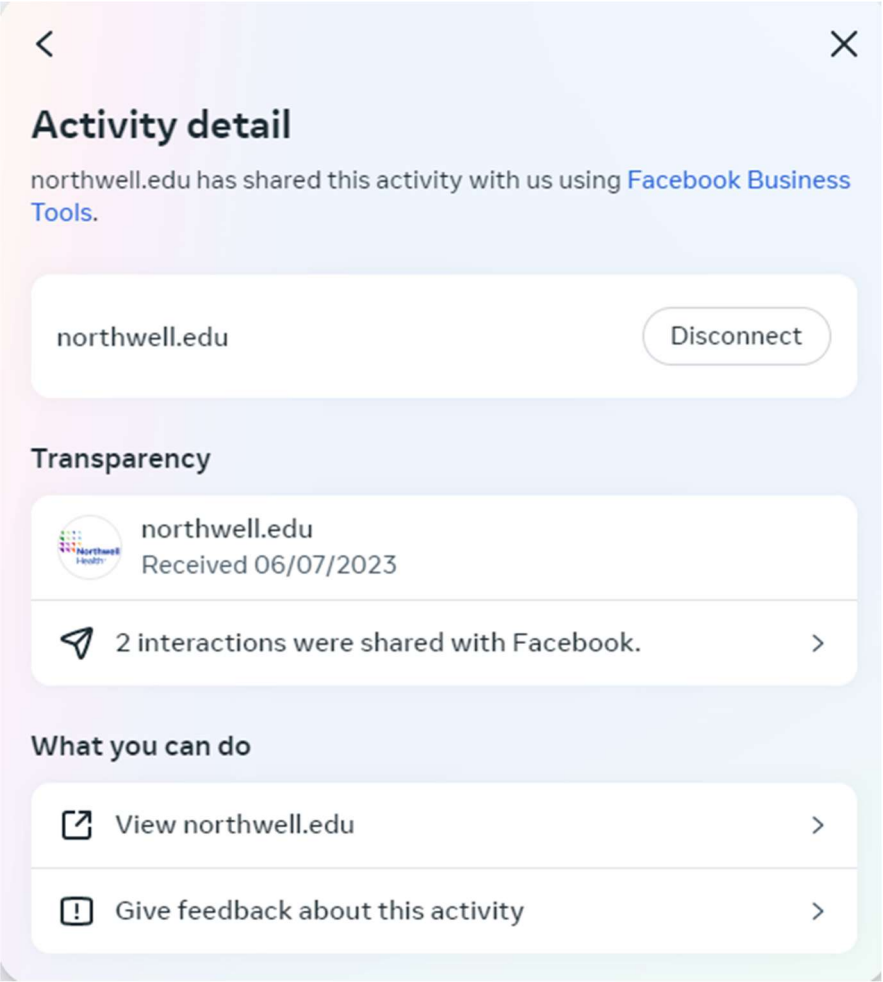
[25] Additional persistent identifiers include Wi-Fi MAC (media access control), Router MAC (a/k/a BSSID) address; IMEI (International Mobile Equipment Identity); AAID (android advertising ID); Hardware ID (serial number); and Router SSID (Service Set ID). Notably, the FTC has found that MAC addresses alone are considered personally identifiable information under the Children's Online Privacy Protection Act.

Name	Value	Domain	Path	Expires / Max-Age
fr	0WL0FIWJOpJ7zUvBn.AWUYSk665Y7v...	.facebook.com	/	2023-11-29T14:16:42.858Z
xs	8%3A3dFkCytZbUSy_w%3A2%3A1671...	.facebook.com	/	2024-08-30T14:16:42.858Z
wd	1817x969	.facebook.com	/	2023-09-07T14:16:45.000Z
c_user	15057[redacted]	.facebook.com	/	2024-08-30T14:16:42.858Z
presence	C%7B%22t3%22%3A%5B%5D%2C%22...	.facebook.com	/	Session
sb	ZTEtYZZxSmecdPr7BegRtryb	.facebook.com	/	2024-01-26T17:04:25.613Z
AWSALBTGCORS	/5oGHNzS49wo9agdADKL4yN/H2LwR...	northwell.us-4.evergage.com	/	2023-09-07T16:37:22.587Z
sa-user-id-v3	s%3AAQAKIP4KCGNalQA_sMypoeeRN...	.srv.stackadapt.com	/	2024-07-26T16:12:01.539Z
apiDomain_3_L3IXuO7...	socialize.sherwin-williams.com	.cdns.us1.gigya.com	/	2024-08-20T20:04:02.000Z
gig_canary_3_e2Uo1F...	false	.cdns.us1.gigya.com	/	2024-08-30T16:37:23.000Z
gig_canary_3_L3IXuO7...	false	.cdns.us1.gigya.com	/	2024-08-20T20:02:18.000Z
_ga_JVWJWV4T9S	GS1.1.1693499841.3.1.1693499844.0.0.0	.northwell.edu	/	2024-10-04T16:37:24.297Z
_ga	GA1.1.283724749.1693245185	.northwell.edu	/	2024-10-04T16:37:24.285Z
ai_session	RXDA6mYQW7TIX/0aDE1yn3|1693495...	www.northwell.edu	/	2023-08-31T17:07:23.676Z
sa-user-id-v3	s%3AAQAKIP4KCGNalQA_sMypoeeRN...	tags.srv.stackadapt.com	/	2024-07-26T16:12:01.538Z
_gat_UA-56792671-30	1	.northwell.edu	/	2023-08-31T16:38:23.000Z
sessionPageCount	1	.northwell.edu	/	2023-08-31T17:07:23.000Z
sa-user-id-v2	s%3Ax6eUGX_DX1dJuy6UaAPFo8wdD...	.srv.stackadapt.com	/	2024-06-11T20:41:36.690Z
gig_canary_ver	15304-3-28224990	.www.northwell.edu	/	Session
apiDomain_3_e2Uo1F...	8065684-gigya.northwell.edu	.cdns.us1.gigya.com	/	2024-08-30T16:37:23.000Z
_fbp	fb.2.1693495769250.763027500	.www.northwell.edu	/	2023-11-29T16:37:24.000Z
incap_ses_483_2973726	Y0rIMxcHFGw+y1X5/vazBsHB8GQAAA...	.northwell.edu	/	Session
_gid	GA1.2.1772889351.1693495769	.northwell.edu	/	2023-09-01T16:37:23.000Z
sa-user-id	s%3A0-8d40b89f-a91e-430b-7544-13...	tags.srv.stackadapt.com	/	2023-12-27T19:38:58.053Z
gig_canary_ver_3_e2Uo...	15304-3-28224990	.cdns.us1.gigya.com	/	2024-08-30T16:37:23.000Z
FPLC	2dBg%2FSrKRcnQ5XUTTE%2Bm2RjXEc...	.northwell.edu	/	2023-08-31T16:57:57.365Z
NW_FPID	FPID2.2.Zesa8pcoA9E%2FW2RvEp6p8...	.northwell.edu	/	2024-10-04T16:37:25.063Z
_mkto_trk	id:309-LVL-470&token:_mch-northwell...	.northwell.edu	/	2024-10-04T16:37:24.087Z
sa-user-id-v2	s%253Ax6eUGX_DX1dJuy6UaAPFo8wd...	www.northwell.edu	/	2024-08-27T17:53:05.000Z
_fbp	fb.1.1693245185332.1257284553	.northwell.edu	/	2024-10-03T20:57:58.450Z
gig_bootstrap_3_FTxaS...	8065684-gigya_ver4	.northwell.edu	/	2024-08-27T17:53:05.000Z
sa-user-id	s%253A0-8d40b89f-a91e-430b-7544-...	www.northwell.edu	/	2024-08-27T17:53:05.000Z
datr	MpMvYdsZU8zEGGmK6YMdLoLJ	.facebook.com	/	2023-11-22T14:48:11.400Z
sa-user-id-v3	s%253AAQAKIP4KCGNalQA_sMypoee...	www.northwell.edu	/	2024-08-27T17:53:05.000Z

93. Importantly, the _fbp cookie is transmitted to Facebook even when the user's browser is configured to block third-party tracking cookies because, unlike the fr cookies and the c_user cookie, the _fbp cookie functions as a first-party cookie—i.e., a cookie that was created and placed on the Website by Defendant.

94. In summation, at a minimum, Facebook uses the fr, _fbp, and c_user cookies to identify specific individuals, and, because the Pixel is automatically programmed to transmit data via both first-party and third-party cookies, proactively disabling third-party cookies will not prevent patients from being individually identified by Facebook and other third-parties with whom Defendant shares data for purposes of marketing and monetization.

95. The image below, taken from a user's own Facebook account after the fact, makes it patently clear that Defendant was actively sending patient communications to Facebook, stating "northwell.edu has shared this activity with us using Facebook Business Tools."



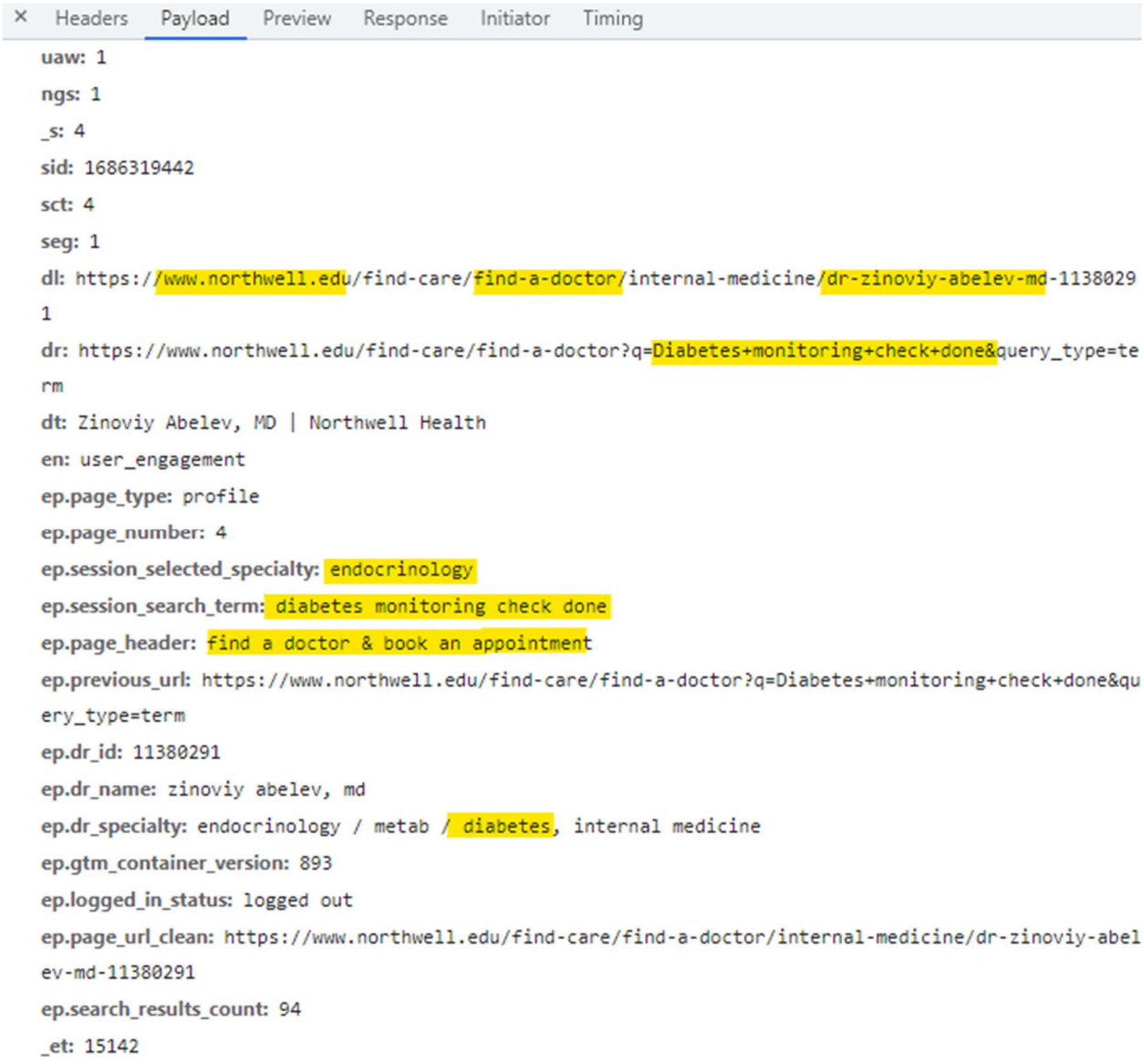
96. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but it is using additional tracking technologies that enable the interception and dissemination of patients' Private Information.

97. For example, Defendant's use of Google Analytics is also problematic, and other healthcare providers have sent data breach notification letters to patients who used digital platforms outfitted with these tools. Like Facebook, Google receives the contents of patients'

communications alongside data that individually identifies anyone with an existing Google account such as an email address "Gmail" or YouTube account.

98. The image below shows what happens when Plaintiffs and other patients use Defendant's website to locate their physician in relation to treatment for a specific medical condition.

99. Defendant does not enable the anonymize feature provided by Google Analytics because the text "aip:" does not appear in the image.



100. Accordingly, Google receives patients' communications searching for specific medical conditions alongside the patients' IP address, which is also impermissible under HIPAA, and device identifiers. Based on their use of the Website, Plaintiffs' communications were also sent to Google, thereby linking their Private Information to other information that allows Google to identify them.

101. Defendant does not disclose that the Tracking Tools, CAPI, cookies, or any other tracking tools embedded in the Website's source code tracks, records, and transmits Plaintiffs' and Class Members' Private Information to Facebook, Google, and/or other third parties who monetize that data for commercial and marketing purposes. Moreover, Defendant never received consent or written authorization to disclose Plaintiffs' and Class Members' private communications to any third party, including Facebook or Google.

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

Plaintiff Eryn Kaplan

102. As a condition of receiving Defendant's services, Plaintiff Kaplan disclosed her Private Information to Defendant as recently as the summer of 2020.

103. Plaintiff Kaplan accessed Defendant's Website on her phone and computer to receive healthcare services from Defendant and, at Defendant's direction, Plaintiff Kaplan also accessed and used Northwell's Patient Portal.

104. Plaintiff Kaplan scheduled doctor's appointments for herself via the Defendant's Website.

105. Plaintiff Kaplan also disclosed information about her specific medical conditions including but not limited to anxiety, panic attacks, and a genetically transmitted syndrome, and

treatments sought, including but not limited to, mental health and genetic testing services, to Defendant by using the Website.

106. Plaintiff Kaplan has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

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

108. Plaintiff Kaplan provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

109. As described herein, Defendant worked along with Facebook to intercept Plaintiff Kaplan's communications, including those that contained Private and confidential information.

110. Defendant willfully facilitated these interceptions without Plaintiff Kaplan's knowledge, consent or express written authorization.

111. Defendant transmitted to Facebook Plaintiff Kaplan's Facebook ID, computer IP address, location, and information such as medical symptoms, conditions and treatment sought, appointment type, physician selected, and button/menu selections.

112. By doing so without her consent, Defendant breached Plaintiff Kaplan's right to privacy and unlawfully disclosed Plaintiffs Kaplan's Private Information.

113. Defendant did not inform Plaintiff Kaplan that it had shared her Private Information with Facebook.

114. After disclosing her private medical information to Defendant, Plaintiff Kaplan began receiving targeted ads on her social media accounts such as Facebook, including ads related to her specific conditions, treatments, and her medical diagnosis.

Plaintiff Michael Zurl

115. As a condition of receiving Defendant's services, Plaintiff Zurl disclosed his Private Information to Defendant as recently as March 2023.

116. Plaintiff Zurl accessed Defendant's Website on his phone and computer to receive healthcare services from Defendant and at Defendant's direction.

117. Plaintiff Zurl scheduled doctor's appointments for himself via the Defendant's Website.

118. Plaintiff Zurl also disclosed information about his specific medical conditions including but not limited to hiatal hernia, swelling of the ankle due to statin medications, and his COVID-19 status, and treatments sought, including but not limited to, hernia and vascular surgery, to Defendant by using the Website.

119. Plaintiff Zurl has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

120. Plaintiff Zurl reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

121. Plaintiff Zurl provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

122. As described herein, Defendant worked along with Facebook, Google, and other third parties to intercept Plaintiff Zurl's communications, including those that contained Private and confidential information.

123. Defendant willfully facilitated these interceptions without Plaintiff Zurl's knowledge, consent, or express written authorization.

124. Defendant transmitted to Facebook Plaintiff Zurl's Facebook ID, computer IP address, location and information such as medical symptoms, conditions and treatment sought, appointment type, physician selected, and button/menu selections.

125. By doing so without his consent, Defendant breached Plaintiff Zurl's right to privacy and unlawfully disclosed his Private Information.

126. Defendant did not inform Plaintiff Zurl that it had shared his Private Information with Facebook, Google, or other third parties.

127. After disclosing his private medical information to Defendant, Plaintiff Zurl began receiving targeted ads on his social media accounts such as Facebook, including those related to his medications, conditions, treatments, and his specific medical diagnosis.

Plaintiff Kathyann McClendon

128. Plaintiff McClendon has been a patient of Northwell Health since 2006 and has received healthcare services at its hospitals and clinics.

129. On numerous occasions, Plaintiff McClendon accessed and used several features on Defendant's Website in order to receive medical healthcare services from Defendant and its affiliates, and she did so at Defendant's direction, and with Defendant's encouragement.

130. More specifically, Plaintiff McClendon used the tools on the Website to search for and identify neurosurgeons and other medical professionals for the specific purpose of scheduling and obtaining medical treatment in relation to neurological symptoms she was experiencing and treatment for specific medical conditions, including Lyme Disease.

131. In doing so, she communicated specific details related to her own medical symptoms which, at the time, were indicative of brain tumors and related neurological disorders.

132. Additionally, Plaintiff McClendon has used Defendant's Website several times per year to book appointments for her medical conditions.

133. Plaintiff McClendon has been an active Facebook user since at least 2004, and she regularly accessed her account from the same devices that she used to access Defendant's Website.

134. Following her visits to Defendant's Website, Plaintiff viewed targeted advertisements on her Facebook account that were related to the symptoms and conditions she communicated via Defendant's website, the specific treatments she sought, and the doctors and specialists she identified and obtained treatment from.

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

136. Plaintiff McClendon provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

137. As described herein, Defendant worked along with Facebook, Google, and other third parties to intercept Plaintiff McClendon's communications, including those that contained Private and confidential information.

138. Defendant willfully facilitated these interceptions without Plaintiff McClendon's knowledge, consent, or express written authorization.

139. Defendant transmitted to Facebook Plaintiff McClendon's Facebook ID, computer IP address, location and information such as medical symptoms, conditions and treatment sought, appointment type, physician selected, and button/menu selections.

140. By doing so without his consent, Defendant breached Plaintiff McClendon's right to privacy and unlawfully disclosed her Private Information.

141. Defendant did not inform Plaintiff McClendon that it had shared her Private Information with Facebook, Google, or other third parties.

Plaintiffs' Experiences Summary

142. After intercepting and collecting this information from Defendant, 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.

143. Based on the presence of the Pixel and Conversions API, Defendant unlawfully disclosed Plaintiffs' Private Information to Facebook. The presence of Facebook advertisements confirms Defendant's unlawful transmission of Plaintiffs' Private Information to Facebook. Said differently, Plaintiffs did not disclose this Private Information to any other source—only Defendant's Website.

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

145. Defendant breached Plaintiffs' right to privacy and unlawfully disclosed their Private Information to Facebook. Specifically, Plaintiffs had a reasonable expectation of privacy,

based on their status as Defendant's patient, that Defendant would not disclose their Private Information to third parties.

146. Defendant did not inform Plaintiffs that it shared their Private Information with Facebook.

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

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

149. Plaintiffs suffered injuries in the form of (i) invasion of privacy; (ii) loss of the benefit of the bargain; (iii) diminution of value of the Private Information; (iv) statutory damages; and (v) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiffs' medical conditions and other confidential information they communicated to Defendant via the Website.

150. Plaintiffs have a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure. As of the filing of the original Complaint on September 27, 2023, Defendant continued to have the Facebook Pixel embedded on its Website, including on its Find a Doctor webpage.[26] While there does not seem to be a Facebook Pixel present on Defendant's Website at the present moment, there is no guarantee that Defendant will not decide to embed this tracking code again. In addition, upon information

[26] *See* https://www.northwell.edu/find-care.

and belief, Defendant has not retrieved from Facebook, Google, or other third parties Plaintiffs' HIPAA-protected Private Information, or caused those third parties to destroy the information they improperly received.

G. Defendant's Conduct Is Unlawful and Violated Industry Norms.

i. Defendant Violated HIPAA Standards.

151. 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]

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

153. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[28]

154. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

155. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider,

[27] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[28] HHS.gov, HIPAA For Professionals, https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html.

health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

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

> a. Names;
>
> ***
>
> H. Medical record numbers;
>
> ***
>
> J. Account numbers;
>
> ***
>
> M. Device identifiers and serial numbers;
>
> N. Web Universal Resource Locators (URLs);
>
> O. Internet Protocol (IP) address numbers; … and
>
> R. Any other unique identifying number, characteristic, or code…;and"
>
> The covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 160.514.

157. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health

information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

158. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6.

159. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Advocate when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

160. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both."

161. 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.[29]

162. 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 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).[30]

163. Defendant's actions violated HIPAA Rules. While there is no private right of action under HIPAA and these violations do not constitute a cause of action in and of themselves, the violation of HIPAA Rules provides context for the elements of Plaintiffs' and Class Members' underlying claims, including, *inter alia*: (1) the confidential nature of the information communicated to Defendant; (2) Plaintiffs' and Class Members' reasonable expectation of privacy in their confidential Private Information; (3) the highly offensive nature of Defendant's disclosure of Private Information; and (4) the fact that the Private Information communicated (including searches for specific symptoms, health conditions, or doctors or the scheduling of appointments) constitutes the "contents" of the communication.

[29]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.
[30]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

ii. Defendant Violated New York Law.

164. New York law has established policies and procedures for the maintenance, preservation, and storage of patient medical records.

165. New York law provides that all patients are entitled to privacy and confidentiality with respect to their treatment and medical records: "[e]very patient shall have the right to have privacy in treatment and in caring for personal needs, confidentiality in the treatment of personal and medical records, and security in storing personal possessions." N.Y. Pub. Health Law § 2803(3)(f).

166. New York law also provides that medical professionals are not allowed to disclose information obtained from a patient: "[u]nless the patient waives the privilege, a person authorized to practice medicine, registered professional nursing, licensed practical nursing, dentistry, podiatry or chiropractic shall not be allowed to disclose any information which she acquired in attending a patient in a professional capacity, and which was necessary to enable her to act in that capacity." N.Y. C.P.L.R. 4504.

167. Defendant's actions described herein violated New York law.

iii. Defendant Violated Industry Standards.

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

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

170. 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)

171. 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.

172. 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.

173. Defendant's violations of industry standards regarding the privacy and confidentiality of patient data and communications provide context for the elements of Plaintiffs' and Class Members' underlying claims, including, *inter alia*: (1) the confidential nature of the information communicated to Defendant; (2) Plaintiffs' and Class Members' reasonable expectation of privacy in their confidential Private Information; (3) the highly offensive nature of Defendant's disclosure of Private Information; and (4) the fact that the Private Information communicated (including searches for specific symptoms, health conditions, or doctors or the scheduling of appointments) constitutes the "contents" of the communication.

H. ***Plaintiffs' and Class Members' Expectation of Privacy.***

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

175. Indeed, at all times when Plaintiffs 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.

176. Plaintiffs and Class Members would not have used Defendant's Website, would not have provided their Private Information to Defendant, and would not have paid for Defendant's healthcare services, or would have paid less for them, had they known that Defendant would disclose their Private Information to third parties.

I. IP Addresses Are Personally Identifiable Information.

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

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

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

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

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

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

183. 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).

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

J. Defendant Was Enriched and Benefitted from the Use of The Tracking Tools and the Unauthorized Disclosures that Resulted from Their Use.

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

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

187. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients to use its services. Defendant did so through use of the intercepted patient data it obtained, procured, and/or disclosed in the absence

of express written consent. Each of the Plaintiffs received such unwanted targeted advertising following their use of Defendant's Website.

188. By utilizing the Tracking Tools, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby benefitting Defendant while invading the privacy of Plaintiffs and Class Members and violating their rights under federal and New York law.

K. Plaintiffs' and Class Members' Private Information Had Financial Value.

189. Plaintiffs' 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. Google similarly uses data to sell advertising. Google has recognized the value of user data and has even instituted a pilot program in which it pays users $3 per week to track them online.

190. 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.

191. 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]

[31] *See* https://time.com/4588104/medical-data-industry/.

192. 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]

193. Indeed, numerous marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. "No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable."[33]

194. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig*., 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

195. Several companies have products through which they pay consumers for a license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing historical information.

196. Facebook also has paid users for their digital information, including browsing history. Until 2019, Facebook ran a "Facebook Research" app through which it paid $20 a month

[32] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

[33] VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER https://www.getvero.com/resources/twitter-lead-generation-cards/.

for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

197. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to $250 per record on the black market.[34]

TOLLING

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

CLASS ACTION ALLEGATIONS

199. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") pursuant to N.Y. C.P.L.R. 901.

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

> All individuals residing in the United States who are, or were, patients of Defendant or any of its affiliates, used Defendant's Website and had their Private Information disclosed to a third party without authorization.

In the alternative, Plaintiffs seek to represent a "New York Class" defined as:

> All individuals residing in New York who are, or were, patients of Defendant or any of its affiliates, used Defendant's Website, and had their Private Information disclosed to a third party without authorization or consent.

The Nationwide Class and New York Class are collectively referred to as the "Class."

201. 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

[34] Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data, SecureLink* (June 30, 2021), https://www.securelink.com/blog/healthcare-data-new-prize-hackers.

successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

202. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

203. Numerosity, N.Y. C.P.L.R 901(a)(1): The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are thousands of individuals whose PII and PHI may have been improperly disclosed to Facebook, and the Class is identifiable within Defendant's records.

204. Commonality, N.Y. C.P.L.R 901(a)(2): 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 Plaintiffs and Class Members;

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

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

d. Whether Defendant violated the law by failing to promptly notify Plaintiffs 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 Plaintiffs and Class Members;

g. Whether Defendant's conduct violated the New York Deceptive Trade Practices Act, Gen. Bus. Law § 349;

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

i. Whether Plaintiffs 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.

205. Typicality, N.Y. C.P.L.R 901(a)(3):. Plaintiffs' 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.

206. Adequacy, N.Y. C.P.L.R 901(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

207. Superiority and Manageability, N.Y. C.P.L.R 901(a)(5): 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.

208. Policies Generally Applicable to the Class. 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 Plaintiffs' 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 Plaintiffs.

209. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs 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 Plaintiffs were 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.

210. 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.

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

212. 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.

213. 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 N.Y. C.P.L.R § 901(b), which permits class actions where appropriate injunctive or declaratory relief may be awarded to an entire class.

214. Issue Certification. 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 Plaintiffs' and Class Members' Private Information;

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

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to disclosure of Plaintiffs' and Class Members' Private Information;

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

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

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

CLAIMS

COUNT I

BREACH OF FIDUCIARY DUTY/CONFIDENTIALITY
(On Behalf of Plaintiffs and the Class)

215. Plaintiffs incorporate all prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

216. Medical providers have a duty to their patients to keep non-public medical information completely confidential, and to safeguard sensitive personal and medical information. This duty arises from the implied covenant of trust and confidence that is inherent in the physician-patient relationship.

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

218. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became a guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members: (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of disclosure of their Private Information to unauthorized third parties; and (3) to maintain complete and accurate records of what patient information (and where) Defendant did and does store and disclose.

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

220. These disclosures were made for commercial purposes without Plaintiffs' or Class Members' knowledge, consent, or authorization, and were unprivileged.

221. The unauthorized disclosures of Plaintiffs' and Class Members' Private Information were intentionally caused by Defendant's employees acting within the scope of their employment. Alternatively, the disclosures of Plaintiffs' and Class Members' Private Information occurred because of Defendant's negligent hiring or supervision of its employees, its failure to establish adequate policies and procedures to safeguard the confidentiality of patient information, or its failure to train its employees to properly discharge their duties under those policies and procedures.

222. The third-party recipients included, but may not be limited to, Facebook and Google. Such information was received by these third parties in a manner that allowed them to identify the Plaintiffs and the individual Class Members.

223. Defendant's breach of the common law implied covenant of trust and confidence is evidenced by its failure to comply with federal and state privacy regulations, including:

a. by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

c. failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);

d. failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiffs' and Class Members' PHI;

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in violation of 45 C.F.R. § 164.312(e)(1);

g. impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq.*;

h. failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5);

i. failing to keep Private Information confidential as required by N.Y. C.P.L.R. 4504;

j. failing to keep Private Information confidential as required by N.Y. Pub. Health Law § 2803(3)(f); and

k. Failing to keep Private Information confidential as required by N.Y. Pub. Health Law § 4410(2).

224. The harm arising from a breach of provider-patient confidentiality includes mental suffering due to the exposure of Private Information and erosion of the essential confidential relationship between the healthcare provider and the patient.

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

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

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

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

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

e. Nominal damages for each independent violation;

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

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

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

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

COUNT II

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

226. Plaintiffs incorporate the prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

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

228. 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.

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

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

231. **Electronic Communications**. The transmission of Private Information between Plaintiffs 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).

232. **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).

233. **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).

234. **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. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' 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

235. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Pixel imbedded and ran on its Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiffs' and Class Members' electronic communications to third parties, including Facebook and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

236. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Tracking Pixel embedded on its Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiffs' and Class Members' electronic communications, for purposes other than providing health care services to Plaintiffs and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

237. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the source code embedded on its Website, contemporaneously and intentionally redirected the contents of Plaintiffs' and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

238. Defendant's intercepted communications include, but are not limited to, the contents of communications to/from Plaintiffs' and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

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

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

241. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

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

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

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

245. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State – namely, violations of HIPAA, the New York Patient's Bill of Rights, New York Public Health laws, and invasion of privacy, among others.

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

247. Defendant is a "party to the communication" with respect to patient communications. However, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiffs' and Class Members' Private Information does not qualify for the party exemption.

248. Defendant's acquisition of patient communications that were used and disclosed to Facebook and Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and New York, including.

a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;
b. Criminal violation of New York Computer Crime statutes, including: Unauthorized use of computer (N.Y. Penal § 156.05); Unlawful duplication (N.Y. Penal § 156.29); and Computer trespass (N.Y. Penal § 156.10);
c. Violation of the New York Patient's Bill of Rights, N.Y. Pub. Health § 2803-c;
d. Violation of law regarding New York Civil Practice Law and Rules § 4504;
e. Violation of the New York Deceptive Trade Practices Act, Gen. Bus. Law § 349; and
f. Invasion of Privacy.

249. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person … without authorization" from the patient.

250. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

251. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it:

a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and

b. Disclosed individually identifiable health information to Facebook and Google without patient authorization.

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

253. Under N.Y. Penal § 156.05, a person commits the offense of unauthorized use of a computer if he "knowingly uses, causes to be used, or accesses a computer, computer service, or computer network without authorization."

254. Defendant violated the N.Y. Penal § 156.05 in that Defendant knowingly used and accessed Plaintiffs' and Class Members' computing devices and data as part of a deception and without their authorization, including through placement of the fbp, ga, and gid cookies as well as use of source code that commanded Plaintiffs' and Class Members' computing devices to send identifiers and the content of communications with Defendant simultaneously to Defendant and Facebook, Google, and others.

255. Under N.Y. Penal § 156.29, a person commits the offense of unlawful duplication of computer related materials if he copies, reproduces or duplicates in any manner computer material that contains records of the medical history or medical treatment of an identified or readily

identifiable individual or individuals with an intent to commit or further the commission of any crime under this chapter.

256. Defendant violated N.Y. Penal § 156.29 by exceeding its authorization to access Plaintiffs' and Class Members' computers including through placement of the fbp, ga, and gid cookies as well as use of source code that commanded Plaintiffs' and Class Members' computing devices to make unauthorized copies of Plaintiffs' and Class Members' electronic data and to send identifiers and the content of communications with Defendant simultaneously to Defendant and Facebook, Google, and others.

257. Under N.Y. Penal § 156.10, a person commits the offense of computer trespass if he knowingly uses, causes to be used, or accesses a computer, computer service, or computer network without authorization and:

a. He or she does so with an intent to commit or attempt to commit or further the commission of any felony; or

b. He or she thereby knowingly gains access to computer material.

258. Defendant violated N.Y. Penal § 156.10 when it knowingly and without Plaintiffs' or Class Members' authorization inserted the fbp, ga, and gid cookies on Plaintiffs' and Class Members' computing devices.

259. The fbp, ga, and gid cookies, which constitute programs, commanded Plaintiffs' and Class Members' computing devices to remove and redirect their data and the content of their communications with Defendant to Google, Facebook, and others.

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

261. Under the New York's Rights of Patients in Certain Medical Facilities, N.Y. Pub. Health § 2803-c(3)(f), "[e]very patient shall have the right to have privacy in treatment and in caring for personal needs, confidentiality in the treatment of personal and medical records, and security in storing personal possessions."

262. Defendant violated the New York Rights of Patients by disclosing Plaintiffs' and Class Members' Private Information to third parties without authorization or consent.

263. Under New York Civil Practice Law and Rules Section 4504, "[u]nless the patient waives the privilege" medical professionals are not "allowed to disclose any information which he acquired in attending a patient in a professional capacity, and which was necessary to enable him to act in that capacity."

264. Defendant violated N.Y. C.P.L.R. 4504 by disclosing Plaintiffs' and Class Members' Private Information to third parties without authorization or consent.

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

266. Defendant accessed, obtained, and disclosed Plaintiffs' and Class Members' Private Information for the purpose of committing the crimes and torts described herein because it

would not have been able to obtain the information or the marketing services if it had complied with the law.

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

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

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

b. Defendant received substantial financial benefits from its use of Plaintiffs' and Class Members' individually identifiable patient health information without providing any value or benefit to Plaintiffs or the Class Members;

c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and Class Members' individually identifiable patient health information, such as understanding how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiffs or the Class Members;

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

e. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as

patient status, test results, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

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

COUNT III

INVASION OF PRIVACY
Violations of N.Y. Civ. Rights Laws §§ 50, 51
(On Behalf of Plaintiffs and the Class)

270. Plaintiffs incorporate the prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

271. Plaintiffs and Class Members have a statutory privacy interest in their names, portraits, pictures, and voices under New York law.

272. Defendant knowingly used Plaintiffs' and Class Members' names and other Private Information in the State of New York for advertising and trade purposes without first obtaining their written consent.

273. Specifically, Defendant transmitted Plaintiffs' and Class Members' names and/or FID to third parties like Facebook for targeted online advertising and other commercial purposes, as described herein.

274. Defendant's use of Plaintiffs' and Class Members' names and Private Information did not serve any public interest.

275. The unlawful tracking of Plaintiffs and Class Members and disclosure of their names in connection with their Private Information has caused Plaintiffs and Class Members to

suffer damages. This includes damage to the value of their information, which Defendant appropriated for its own enrichment. Plaintiffs and Class Members have also suffered nominal damages.

276. Defendant failed to protect Plaintiffs' 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.

277. 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 Plaintiffs and Class Members.

278. Plaintiffs, on behalf of herself and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, plus prejudgment interest, and costs. Alternatively, Plaintiffs and Class Members are entitled to nominal damages.

279. Plaintiffs and Class Members are entitled to exemplary and/or punitive damages as a result of Defendant's knowing violations of their statutory rights to privacy.

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

281. Plaintiffs 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.

282. Plaintiffs, on behalf of herself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into Plaintiffs' and Class Members' statutory privacy interests.

COUNT IV

BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

283. Plaintiffs incorporate the prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

284. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiffs and the Class Members provided their Private Information and compensation for their medical care.

285. When Plaintiffs 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.

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

287. Plaintiffs and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

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

289. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs 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.

290. Plaintiffs 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 Plaintiffs and the Class)

291. Plaintiffs incorporate the prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

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

293. Plaintiffs and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiffs and Class Members, without authorization and proper compensation to exceed the limited authorization and access to that information which was given to Defendant.

294. Defendant exceeded any authorization given and instead consciously disclosed and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

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

296. The benefits that Defendant derived from Plaintiffs and Class Members were not offered by Plaintiffs and Class Members gratuitously and rightly belongs to Plaintiffs and Class

Members. It would against equity and good conscience 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.

297. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs 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

NEGLIGENCE
(On behalf of Plaintiffs and the Class)

298. Plaintiffs incorporate the prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

299. Defendant owed Plaintiffs and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

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

301. 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 Plaintiffs' and Class Members' communications with Defendant, including Private Information and the contents of such information.

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

303. The third-party recipients included, but may not be limited to, Facebook.

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

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

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

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

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

e. Nominal damages for each independent violation;

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

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

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

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

COUNT VII

VIOLATIONS OF THE NEW YORK CONSUMER LAW FOR DECEPTIVE ACTS AND PRACTICES GEN. BUS. LAW § 349
(On behalf of Plaintiffs and the Class)

305. Plaintiffs incorporate the prior allegations as if fully set forth herein and bring this Count individually and on behalf of the proposed Class.

306. This cause of action is brought pursuant to the New York General Business Law § 349 ("NYGBL"), which New York courts have invariably interpreted using the kind of liberal construction afforded to state consumer protection statutes intended to prevent fraud.

307. NYGBL § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

308. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of NYGBL § 349, and the deception occurred within New York State.

309. By serving as Plaintiffs' and Class Members' healthcare provider, Defendant had a duty to protect their Private Information from unlawful disclosure.

310. Plaintiffs and the Class Members paid for or otherwise availed themselves and received services from Defendant, for the purpose of medical treatment.

311. Defendant engaged in the conduct alleged in this Class Action Complaint, entering into transactions intended to result, and which did result, in the provision of medical treatment to Plaintiffs and Class Members.

312. Defendant's acts, practices, and omissions were done in the course of Defendant's offer of medical treatment, services, and care throughout the state of New York.

313. The unfair, unconscionable, and unlawful acts and practices of Defendant alleged herein, and in particular the decisions regarding the Facebook Pixel and Conversions API, emanated and arose within the state of New York, within the scope of NYGBL § 349.

314. Defendant, operating in and out of New York, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of NYGBL § 349, including but not limited to the following: (a) knowingly promising to protect Plaintiffs' and Class Members' Private Information, (b) knowingly and improperly storing, possessing, using, and/or procuring the interception of, Plaintiffs' and Class Members' Private Information; and (c) knowingly disclosing Plaintiffs' and Class Members' Private Information to third parties, including Facebook.

315. Defendant committed these acts while concurrently representing that it would protect and not unlawfully disclose Plaintiffs' and Class Members' Private Information unless under a legal obligation to do so.

316. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including by not limited to HIPAA, the New York Patient's Bill of Rights, New York computer crime statutes, statutes regarding the confidentiality of medical records, and NYGBL § 349.

317. Defendant knew or should have known that its Website and the cookies and source code thereon was unlawfully wiretapping, intercepting, and disclosing Plaintiffs' and Class Members' Private Information.

318. Plaintiffs have standing to pursue this claim because as a direct and proximate result of Defendant's violations of NYGBL § 349, Plaintiffs and Class Members have been "aggrieved"

by a violation of NYGBL § 349 and bring this action to obtain a declaratory judgment that Defendant's acts or practices violate NYGBL § 349.

319. Plaintiffs also have standing to pursue this claim because, as a direct result of Defendant's knowing violation of NYGBL § 349, Plaintiffs and Class Members have lost money or property in the form monies paid for Defendant's services, diminution in value of their Private Information, as well as loss of the benefit of their bargain with Defendant.

320. Plaintiffs and Class Members are entitled to injunctive relief to protect them from the substantial and imminent risk of future loss of Private Information, including, but not limited to: (a) ordering that Defendant immediately remove any pixel, web beacon, cookie, or other tracking technology that causes the disclosure of Private Information to third parties without consent; (b) ordering that Defendant engage third-party security auditors and internal personnel to ensure Plaintiffs' and Class Members' Private Information is no longer subject to the unlawful practices described in this Complaint; (c) ordering that Defendant purge, delete, and destroy Private Information not necessary for its provisions of services in a reasonably secure manner; (d) ordering that Defendant conduct regular database scans and security checks; (e) ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to properly handle Private Information provided via Defendant's Website; (f) ordering Defendant to meaningfully educate individuals about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps victims should take to protect themselves.

321. Plaintiffs bring this action on behalf of herself and Class Members for the relief requested above and for the public benefit in order to promote the public's interest in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to

protect Plaintiffs, Class Members, and the public from Defendant's unfair methods of competition and unfair, unconscionable, and unlawful practices. Defendant's wrongful conduct as alleged in this Class Action Complaint has had widespread impact on the public at large.

322. The above unfair, unconscionable, and unlawful practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

323. Defendant's actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

324. Plaintiffs and Class Members seek relief under NYGBL § 349, including, but not limited to, a declaratory judgment that Defendant's actions and/or practices violate NYGBL § 349; injunctive relief enjoining Defendant, their employees, parents, subsidiaries, affiliates, executives, and agents from continuing to violate NYGBL § 349 as described above.

325. Plaintiffs and Class Members are also entitled to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, respectfully request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiffs 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 Plaintiffs and Class Members;

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

D. For an award of damages, including, but not limited to, actual, consequential, statutory, 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

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

DATE: June 23, 2025

Respectfully Submitted,

s/: David S. Almeida
David S. Almeida
Elena A. Belov
Karen Dahlberg O'Connell
New York Bar No. 3056520
New York Bar No. 4080891
New York Bar No. 4136339
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
(708) 437-6476
david@almeidalawgroup.com
elena@almeidalawgroup.com
karen@almeidalawgroup.com

Gary M. Klinger*

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Glen Abramson*
Alex M. Honeycutt*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (866-252-0878)
gabramson@milberg.com
ahoneycutt@milberg.com

Bryan L. Bleichner*
Philip J. Krzeski*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.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, LLC
2754 Erie Ave.
Cincinnati, Ohio 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Counsel for Plaintiffs & the Putative Classes

* *pro hac vice* forthcoming

ClassAction.org
