

U.S. DISTRICT COURT
DISTRICT OF VERMONT
FILED

UNITED STATES DISTRICT COURT
DISTRICT OF VERMONT

2024 JUN 20 AM 10: 09

CLERK

TYLER BAKER, *individually and on behalf of
all others similarly situated,*

Plaintiff,

vs.

UNIVERSITY OF VERMONT HEALTH
NETWORK INC. and UNIVERSITY OF
VERMONT MEDICAL CENTER INC.

Defendants.

Case No.: 2:24-cv-673 *BY* *[Signature]*
DEPUTY CLERK

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Tyler Baker (“**Plaintiff**”), individually and on behalf of all others similarly situated, bring this class action lawsuit against Defendants University of Vermont Health Network Inc. and University of Vermont Medical Center Inc. (collectively “**UVM**” or “**Defendants**”). Plaintiff’s allegations are based upon personal knowledge as to themselves and their own acts, and upon information and good faith belief as to all other matters based on the investigation conducted by undersigned counsel.

INTRODUCTION

1. This case seeks legal redress for Defendants’ conscious decision to install tracking technologies on their websites to intercept patients’ personal health information and disclose that highly sensitive information to third party platforms like Facebook and Google without consent.

2. Defendants are for-profit healthcare organizations associated with the University of Vermont. Defendant University of Vermont Health Network Inc. is an integrated academic health network that serves more than one million patients across the state of Vermont and northern

New York, over 1,500 doctors and specialists, and a wide range of medical services offered.¹ Defendant University of Vermont Medical Center Inc. is a five-campus medical facility.²

3. In order to market, sell and provide its healthcare offerings, Defendants own, maintain and operate a website, <https://www.uvmhealth.org> (the “**Website**”).

4. As detailed herein, Defendants disregarded the privacy rights of its patients who used its Website (“**Users**” or “**Class Members**”) by installing, configuring and using pixels and other tracking technologies on its Website to collect and divulge their personally identifiable information (“**PII**”) and protected health information (“**PHI**” and collectively, “**Private Information**”) to Meta Platform Inc. d/b/a Facebook and other social media platforms.

5. Unbeknownst to Users and without their authorization or informed consent, Defendants installed Facebook’s Meta Pixel (“**Meta Pixel**” or “**Pixel**”) and other invisible third-party tracking technology on its Website in order to intercept Users’ PII and PHI with the express purpose of disclosing that Private Information to third parties such as Meta and/or Google LLC in violation of HIPAA Privacy Rule and 42 U.S.C. § 1320d-6 as well as state, federal and common law.

6. Meta then accesses and uses the Private Information by associating it with the individual User whose information was disclosed. Meta is able to personally identify each User with an active Facebook account by using the “c_user” cookie that Meta stores in users’ browsers and which reveals a Facebook account-holder’s unique Facebook ID (“FID”) value.

7. A user’s FID is linked to their Facebook profile which personally identifies the user through a wide range of demographic and other information about the user including the User’s

¹ University of Vermont Health Network, <https://www.uvmhealth.org/>

² The Heart and Science of Medicine, <https://www.uvmhealth.org/medcenter/about-uvm-medical-center>

name, pictures, personal interests, work history, relationship status and other details. Because the user's FID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the FID to quickly and easily locate, access, and view the user's corresponding Facebook profile.³

8. Notably, the Pixel collects data regardless of whether the User has a Facebook account as Facebook maintains “shadow profiles” on users without Facebook accounts and links the information collected via the Pixel to the user's real-world identity using their shadow profile.⁴

9. The screenshots of Defendants' website, more fully explained *infra*, demonstrate how the Meta Pixel intercepts Users' Private Information including the Private Information of Plaintiff and Class Members.

10. Depending on the browser they are using, customers and others can also inspect the “source code” of a particular website (in Google Chrome this can be done by “right-clicking” on a webpage and selecting “inspect” from the menu that appears) to view the performance of the Pixel in order to see what information Defendants is disclosing to Meta for each webpage a User is visiting.

11. Data privacy experts are also capable of viewing how the Meta Pixel operates on various websites, including past configurations, and expert analysis demonstrates how Defendants used the Pixels on their Website, in particular. Below are larger images of the Meta pixel in action. Though it appears to be code, a closer inspection makes it apparent that Defendants are disclosing

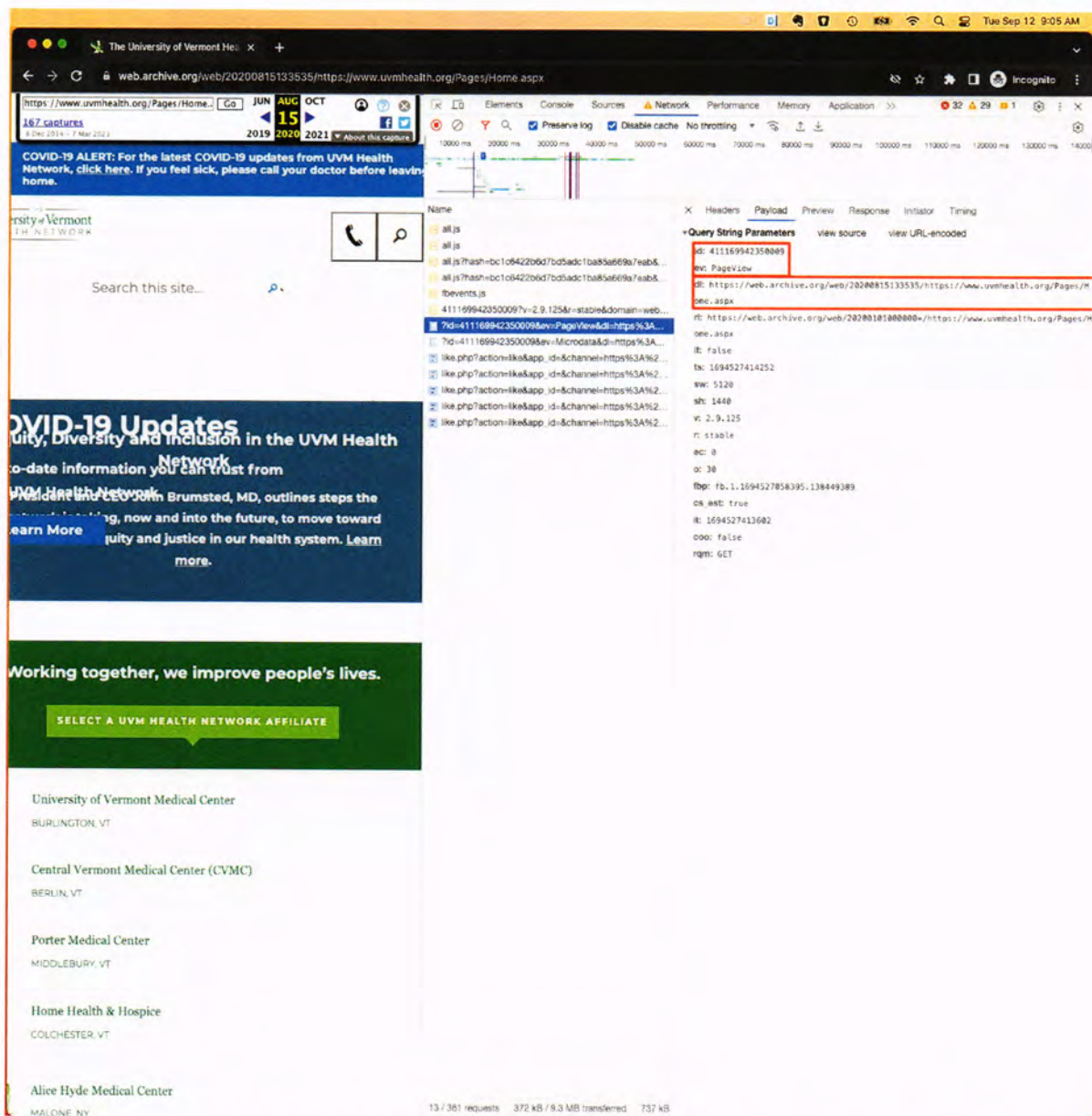
³ To find the Facebook account associated with a particular c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

⁴ See Russell Brandom, *Shadow Profiles Are The Biggest Flaw In Facebook's Privacy Defense*, TheVerge.com (Apr 11, 2018), available at <https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy> (last May 14, 2024).

both personally identifiable information in the form of the c_user FID, which uniquely identifies an individual's Facebook account (as well as other cookies that Facebook is known to utilize to identify individuals).

12. The highlights in the screenshot below show some of the categories of information that Defendants are sharing with Meta. Beginning at the top, the "id=411169942350009" is the unique ID number of one of the Pixels installed by Defendant. Below this is "PageView," a type of 'event' collected by the Pixel as the User navigates the Website which shares the URL of the page that the User is visiting. "dl" shares the pages that the user is visiting with Meta. As shown by the images below and as Plaintiff's research showed, Defendants disclose the descriptive URL of any treatment-specific page visited, type of provider sought, or the fact that the patient is making an appointment.

13. The first screenshot below shows what a webpage from Defendants' Website looks like when you use browser developer tools to see which information the Pixel discloses to Meta.



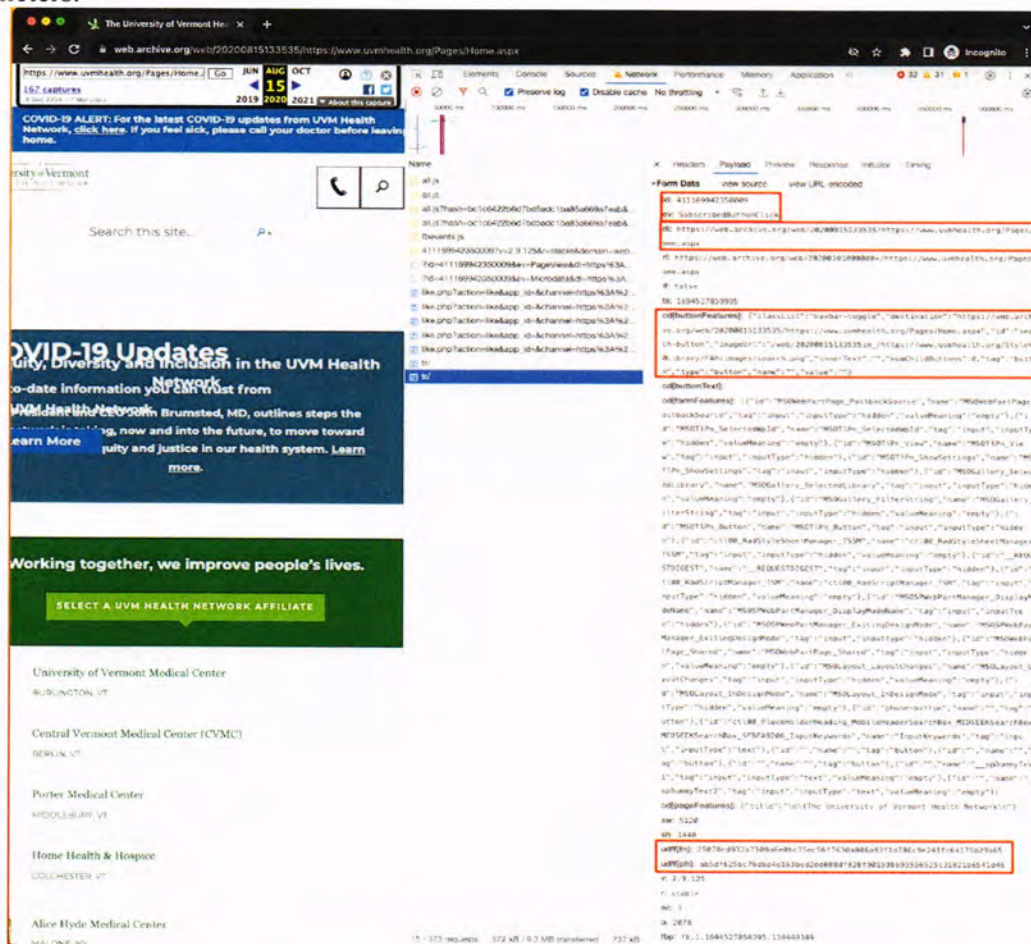
14. On the left-hand side of the screenshot is the page as it appears to any User visiting this webpage. The right-hand side of the screenshot shows the Pixel information as displayed in the browser developer tools.

15. Defendants used the Pixel tool to track users' movements across the site and report it back to Facebook, associating this highly personal data with the user's Facebook account.

16. Analysis revealed that Defendants used two different Pixel configurations,

411169942350009 (“Pixel1”) and 1029632157153338 (“Pixel2”). Pixel tracking was active on the Website from at least July 2016 to September 2023.

17. When a user navigates to browse information about doctors and specialists at UVM, UVM discloses that information to Facebook by sending a `SubscribedButtonClick` and pair of `Pageview` and `Microdata` events upon the user’s clicking to open and launching of the “Doctors & Specialists” link, respectively. The screenshots below illustrate this and Defendants use of the “udff[fn]” and “udff[ph]” parameters, which signify that Defendants enabled Advanced Matching Parameters.⁵



⁵ Advanced Matching Parameters allow Meta to connect event data with user profiles, even if the user has taken steps to avoid Facebook browser cookies, such as by blocking them or using a browser that does not allow them. In this instance, Defendants enabled the Pixels to capture and

18. By using the Pixels they install on their Website, Defendants intercept both the PII and the PHI of every User that visits every webpage, with the specific purpose of disclosing that HIPAA-protected health information to Meta.

19. Meta, which created the Pixel and assigns a unique FID to each of its Facebook account holders, knows how to combine the information intercepted and shared by Defendants so that Meta can connect each User to the PHI that is disclosed. Meta does this in order to send targeted ads related to the medical conditions and treatments each User shares with Defendants to that User's personal Facebook account.

20. The Pixel intercepts and discloses the information of every Facebook user that visits the Defendants' Website in the same way.

21. When Plaintiff and Class Members visited Defendants' Website, the URLs that describe the medical information on each page they visited and/or the search terms they typed in Defendants' search bar were simultaneously shared with Meta during every interaction.

22. And together with that PHI, Defendants' Pixel (which relies on Facebook cookies to function) discloses to Meta the Facebook user ID of every person that visits its Website so that Meta can personally identify that user and that user's PHI – including Plaintiff and every Class Member who visited Defendants' Website to research and share HIPAA-protected health information with Defendants while the Pixel was installed on the Website.

23. Plaintiff and Class Members who visited and used Defendants' Website thought they were communicating with only their trusted healthcare providers, and reasonably believed that their sensitive and private PHI would be guarded with the utmost care. In browsing Defendants' Website—be it to make an appointment, locate a doctor with a specific specialty, find

disclose at least the Users' name (the “udff[fn]” value) and their phone number (the “udff[pn]” value).

sensitive information about their diagnosis, or investigate treatment for their diagnosis—Plaintiff and Class Members did not expect that every search (including exact words and phrases they typed into Defendants’ website search bars), extremely sensitive PHI such as health conditions (e.g., breast cancer or pregnancy), diagnoses (e.g., stroke, arthritis, or AIDS), procedures sought, treatment status, and/or their treating physician, or even their accessing Defendants’ online Portal would be intercepted, captured and otherwise shared with Facebook in order to target Plaintiff and Class Members with ads, in conscious disregard of their privacy rights.

24. Plaintiff continued to have his privacy violated when his Private Information was used to turn a profit by way of targeted advertising related to his respective medical conditions and treatments sought.

25. Defendants knew that by embedding the Meta Pixel on the Website it was permitting Facebook to collect and use Plaintiff’s and Class Members’ Private Information, including sensitive medical information.

26. Defendants (or any third parties) did not obtain Plaintiff’s and Class Members’ prior consent before sharing their sensitive, confidential communications with third parties such as Facebook.

27. Defendants’ actions constitute an extreme invasion of Plaintiff’s and Class Members’ right to privacy and violate federal and state statutory and common law as well as Defendants’ own Privacy Policies that affirmatively and unequivocally state that any personal information provided to Defendants will remain secure and protected.

28. For instance, the privacy policy posted on the UVM website at April 28, 2017 (“Privacy Policy”) states that “We only obtain personal information if you choose to provide it to us.” That same page further states “No Sales of Personal Information. We do not sell any personal

information.”⁶

29. As a result of Defendants’ conduct, Plaintiff and Class Members have suffered injuries, including: (i) invasion of privacy; (ii) lack of trust in communicating with doctors online; (iii) emotional distress and heightened concerns related to the release of Private Information to third parties; (iv) loss of the benefit of the bargain; (v) diminution of value of the Private Information; (vi) statutory damages and (vii) continued and ongoing risk to their Private Information.

30. Plaintiff and Class Members have a substantial risk of future harm, and thus injury in fact, due to the continued and ongoing risk of misuse of their Private Information that was shared by Defendants with unauthorized third parties.

31. Plaintiff seeks, on behalf of himself and a class of similarly situated persons, to remedy these harms and therefore assert the following statutory and common law claims against Defendant: (i) Violation of Electronic Communications Privacy Act, 18 U.S.C. §2511(1), *et seq*; (ii) Breach of Express Contract, (iii) Breach of Implied Duty of Good Faith and Fair Dealing, (iv) Breach of Implied Contract, (v) Negligence; (vi) Breach of Fiduciary Duty; (vii) Unjust Enrichment; and (viii) Violation of the Vermont Consumer Protection Act.

PARTIES

32. Plaintiff Tyler Baker is a Vermont citizen residing in Underhill, Vermont, where he intends to remain indefinitely.

33. Plaintiff was a patient of UVM from at least early 2021 for approximately two years during the relevant time period.

⁶ *The University of Vermont Health Network Web Site Privacy Policy*, <https://web.archive.org/web/20170428064038/https://www.uvmhealth.org/pages/privacy-policy.aspx> (last visited Apr. 16, 2024).

34. Defendants University of Vermont Health Network Inc. is a healthcare service provider. Defendant is incorporated in Vermont with its principal place of business located at 462 Shelburne Road, Burlington, VT, 05401.

35. Defendants University of Vermont Medical Center Inc. is a healthcare service provider. Defendants is incorporated in Vermont with its principal place of business located at 111 Colchester Avenue, Burlington, VT, 05401.

JURISDICTION & VENUE

36. This Court has “federal question” jurisdiction given the federal claims alleged by Plaintiff. This Court also has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332(d), because the amount in controversy for the Class exceeds \$5,000,000 exclusive of interest and costs, there are more than one hundred (100) putative class members defined below, and minimal diversity exists because a significant portion of putative class members are citizens of a state different from the citizenship of at least one Defendant.

37. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District. At least one Plaintiff resides in this District and used Defendants’ Website within this District. Moreover, Defendants received substantial compensation from offering healthcare services in this District, and Defendants made numerous misrepresentations which had a substantial effect in this District, including, but not limited to, representing that Defendants will only disclose Private Information provided to them under certain circumstances, *which do not* include disclosure of Private Information for marketing purposes.

38. Defendants are subject to personal jurisdiction in Vermont because Defendants maintain their principal place of business in Vermont and are authorized to conduct and are conducting business in Vermont.

PLAINTIFF'S EXPERIENCE

39. In early 2021, Plaintiff was diagnosed with [REDACTED] and underwent treatment, including [REDACTED], for approximately two years with UVM. While Plaintiff was receiving treatment, he would routinely visit the Website to research the various doctors working at UVM, his specific medical conditions including [REDACTED] [REDACTED] Plaintiff would also visit the Website to access his MyChart.

40. Plaintiff had been accessing the Website on his cell phone and desktop computer.

41. Plaintiff has used and continued to use the same devices to maintain and access an active Facebook account throughout the relevant period (when Defendants' Pixels were present) in this case.

42. During the relevant time period Plaintiff used Defendants' Website to research doctors [REDACTED], access MyChart, communicate information about the diagnosis and sought treatments of his [REDACTED], and look for Defendants' medical care locations close to his residence. During this period this information was disclosed to Meta and other third parties.

43. Shortly after submitting his protected health information to Defendants, including information concerning his specific medical information, including symptoms and treatments, Plaintiff began to receive spam and ads on Facebook and other social media [REDACTED]
[REDACTED]

44. Upon information and good faith belief, Plaintiff began receiving these ads after his PII and PHI concerning his medical condition was disclosed by Defendants through the Pixel to Meta, including advertisements for medications and prescriptions [REDACTED]

45. Meta viewed and accessed this Private Information so that it could personally identify Plaintiff by connecting the cookies on the Website to Plaintiff's Facebook account. Meta also accesses the PHI disclosed by Defendants so that it can use the specific medical information Plaintiff shared with Defendants to identify specific targeted ads related to Plaintiff's medical condition to send to his Facebook account. After accessing and identifying the specific medical conditions it can target with ads, Meta then shares that information with other unauthorized third parties whose businesses and advertisements are related to those conditions.

46. The full scope of Defendants' interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, Defendant intercepted at least the following communications about Plaintiff's patient status, [REDACTED], treatments and healthcare providers sought, via the following long-URLs or substantially similar URLs that were sent to Meta via the Pixels (and which contain information concerning Plaintiff's specific medical conditions, queries, as well as types of providers and treatments sought):

[REDACTED]

[REDACTED]

[REDACTED]/sleep-apnea

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

47. Contemporaneously with the interception and transmission of the contents of Plaintiff's communications regarding his conditions on the Website, Defendants also disclosed to Meta Plaintiff's unique personal identifiers, including but not limited to, his Facebook ID and IP address.

48. During the relevant time period, when the Defendants' Pixels were present, Plaintiff also utilized Defendants' Patient Portal to review his medical records such as his appointment requests, visit summaries, doctor's notes and his test results.

49. The full scope of Defendants' interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery.

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

51. Plaintiff provided his Private Information to Defendants and trusted that the information would be safeguarded according to Defendants' policies and state and federal law.

52. As described herein, Defendants worked along with Facebook to intercept Plaintiff's communications, including those that contained his Private Information.

53. Defendants willfully facilitated these interceptions without Plaintiff's knowledge, consent or express written authorization.

54. Defendants transmitted to Facebook Plaintiff's Facebook ID, computer IP address and sensitive health information such as his medical symptoms, conditions, treatments sought, physician selected, button/menu selections and/or content typed into free text boxes.

55. By doing so without his consent, Defendants breached Plaintiff's privacy and unlawfully disclosed his Private Information.

56. Defendants did not inform Plaintiff that it had shared his Private Information with Facebook.

57. Plaintiff would not have utilized Defendants' medical services and/or used its Website or would have paid much less for Defendants' services had he known that his Private Information would be captured and disclosed to third parties like Facebook without his consent.

FACTUAL BACKGROUND

A. The Irresponsible Use of Invisible Tracking Codes by Healthcare Providers to Send Meta People's Data for their Advertising Business.

58. Meta operates the world's largest social media company whose revenue is derived almost entirely from selling targeted advertising.

59. The Meta Pixel and other third-party tracking tools collect and transmit information from Defendants that identifies a Facebook user's status as a patient and other health information that is protected by federal and state law. This occurs through tools that Facebook encourages its healthcare Partners to use, including uploading patient lists to Facebook for use in its advertising systems.

60. Meta associates the information disclosed by Defendants via the Meta Pixel with other information regarding the User, using personal identifiers that are transmitted concurrently with other information the Pixel is configured to collect.

61. For Facebook account holders, these identifiers include the "c_user" cookie IDs, which allow Meta to link data to a particular Facebook account. For both Facebook account holders and users who do not have a Facebook account, these identifiers also include cookies that Meta ties to their browser.

62. Realizing the value of having direct access to millions of consumers, in 2007, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming it to be a "completely new way of advertising online" that would allow "advertisers to deliver more tailored and relevant ads."⁷

63. One of its most powerful advertising tools is Meta Pixel, formerly known as Facebook Pixel, which launched in 2015.

64. Ad targeting has been extremely successful due, in large part, to Facebook's ability to target people at a granular level. "Among many possible target audiences, Facebook offers advertisers, [for example,] 1.5 million people 'whose activity on Facebook suggests that they're

⁷ *Facebook Unveils Facebook Ads*, META (November 6, 2007), <https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/>.

more likely to engage with/distribute liberal political content’ and nearly seven million Facebook users who ‘prefer high-value goods in Mexico.’”⁸

65. The Meta Pixel is a free and publicly available “piece of code” that third-party web developers can install on their website to “measure, optimize and build audiences for ... ad campaigns.”⁹

66. Meta describes the Pixel as “a snippet of JavaScript code” that “relies on Facebook cookies, which enable [Facebook] to match ... website visitors to their respective Facebook user accounts.”¹⁰

67. Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel “can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart.”¹¹

68. Meta tells advertisers that the Meta Pixel will improve their Facebook advertising, including by allowing them to:

a. “optimize the delivery of your ads” and “[e]nsure your ads reach the people most likely to take action;” and

b. “create Custom Audiences from website visitors” and create “[d]ynamic ads [to] help you automatically show website visitors the products they viewed on your website—or related ones.”¹²

⁸ Natasha Singer, *What You Don’t Know about How Facebook Uses Your Data* (April 11, 2018), <https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html>.

⁹ *Meta Pixel* (2023), <https://www.facebook.com/business/tools/meta-pixel>.

¹⁰ *Meta Pixel* (2023), <https://developers.facebook.com/docs/meta-pixel/>.

¹¹ *Meta Pixel* (2023), <https://www.facebook.com/business/tools/meta-pixel>.

¹² *Id.*

69. Meta explains that the Pixel “log[s] when someone takes an action on your website” such as “adding an item to their shopping cart or making a purchase,” and the user’s subsequent action:



Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in [Events Manager](#). From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads.

70. The Meta Pixel is customizable and web developers choose the actions the Pixel will track and measure on a particular webpage.

71. Meta advises web developers to place the Pixel early in the source code¹³ for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website.¹⁴

72. Meta’s “Health” division is dedicated to marketing to and servicing Meta’s healthcare “Partners.” Meta defines its “Partners” to include businesses that use Meta’s products,

¹³ Source code is a collection of instructions (readable by humans) that programmers write using computer programming languages such as JavaScript, PHP, and Python. When the programmer writes a set or line of source code, it is implemented into an application, website, or another computer program. Then, that code can provide instructions to the website on how to function. *What is Source Code & Why Is It Important?* (July 19, 2023), <https://blog.hubspot.com/website/what-is-source-code> (last May 14, 2024).

¹⁴ *Meta Pixel: Get Started* (2023), <https://developers.facebook.com/docs/meta-pixel/get-started>.

including the Meta Pixel or Meta Audience Network tools to advertise, market, or support their products and services.

73. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.

74. Healthcare providers like Defendants encourage Plaintiff and Class Members to access and use various digital tools via its Website to, among other things, receive healthcare services, in order to gain additional insights into its Users, improve its return on marketing dollars and, ultimately, increase its revenue.

75. In exchange for installing the Pixels, Facebook provided Defendants with analytics about the advertisements it has placed as well as tools to target people who have visited its Website.

76. Upon information and belief, Defendants and other companies utilized Plaintiff's and Class Members' sensitive information and data collected by the Meta Pixels on Defendants' Website in order to advertise to these individuals later on Meta's social platforms.

77. If healthcare providers, such as Defendants, install the Meta Pixel code as Meta recommends, patients' actions on the provider's website are contemporaneously redirected to Meta.

78. Thus, the Meta "pixel allows Facebook to be a silent third-party watching whatever you're doing,"¹⁵ which in this case included the content of Defendants' patients' communications with its Website, including their PHI.

¹⁵ Jefferson Graham, *Facebook spies on us but not by recording our calls. Here's how the social network knows everything* (Apr. 4, 2020),

79. The Pixel acts as a conduit of information, sending the information it collects to Facebook through scripts running in the User's internet browser, via data packets labeled with PII, including the User's IP address, the Facebook c_user cookie and third-party cookies allowing Facebook to link the data collected by Meta Pixel to the specific Facebook user.¹⁶

80. Facebook's access to use even only some of these data points—such as just a “descriptive” webpage URL—is problematic. As Laura Lazaro Cabrera, a legal officer at Privacy International, explained: “Think about what you can learn from a URL that says something about scheduling an abortion’ . . . ‘Facebook is in the business of developing algorithms. They know what sorts of information can act as a proxy for personal data.’”¹⁷

81. The collection and use of this data raises serious concerns about user privacy and the potential misuse of personal information. For example, when Users browse Defendants' Website, every step of their activity is tracked and monitored. By analyzing this data using algorithms and machine learning techniques, Facebook (and other entities tracking this information) can learn a chilling level of detail about Users' medical conditions, behavioral patterns, preferences, and interests.

<https://www.usatoday.com/story/tech/2020/03/04/facebook-not-recording-our-calls-but-has-other-ways-snoop/4795519002/>.

¹⁶ The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users. See Maciej Zawadziński & Michal Wlosik, *What Facebook's First-Party Cookie Means for AdTech* (June 8, 2022), <https://clearcode.cc/blog/facebook-first-party-cookie-adtech/>.

¹⁷ Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, THE MARKUP (Sept. 25, 2022), <https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients>.

82. This data can be used not only to provide personalized and targeted content and advertising, but also for more nefarious purposes, such as tracking and surveillance. Moreover, the misuse of this data could potentially lead to the spread of false or misleading information, which could have serious consequences, particularly in the case of health-related information.

83. As pointed out by the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS), impermissible disclosures of such data in the healthcare context “may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual’s PHI.... This tracking information could also be misused to promote misinformation, identity theft, stalking, and harassment.”¹⁸

84. Unfortunately, several recent reports detail the widespread use of third-party tracking technologies on hospitals’, health care providers’ and telehealth companies’ digital properties to surreptitiously capture and to disclose their Users’ Private Information.¹⁹ Estimates are that over 664 hospital systems and providers utilize some form of tracking technology on their digital properties.²⁰

¹⁸ *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited Mar. 12, 2024).

¹⁹ The Markup reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor’s appointment. Todd Feathers, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, *supra*, note 16.

²⁰ Dave Muoio & Annie Burky, *Advocate Aurora, WakeMed get served class action over Meta’s alleged patient data mining*, FIERCE HEALTHCARE (November 4, 2022), <https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-patient-data-facebook>.

B. Defendants Disclosed Patient Healthcare Information, Including Patient Status, in Violation of the HIPAA Privacy Rule.

85. Healthcare entities collecting and disclosing users' Private Information face significant legal exposure under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which applies specifically to healthcare providers, health insurance providers and healthcare data clearinghouses.²¹

86. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information ("IIHI") that is held or transmitted.²² This is information that can be used to identify, contact, or locate a single person or can be used with other sources to identify a single individual.

87. Plaintiff's IIHI captured by the Pixel and sent to Meta included their unique personal identifiers such as their Facebook ID, IP address, device identifiers and browser "fingerprints."

88. Defendants further violated the HIPAA Privacy Rule, among other statutory and common laws, because Plaintiff's PHI concerning his specific medical conditions (such as Plaintiff's [REDACTED]) was disclosed to Meta by the Pixels and other third-party trackers embedded by Defendants on their Website.

²¹ *Health Information Privacy* (Mar. 31, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>.

²² The HIPAA Privacy Rule protects all electronically protected health information a covered entity like Defendants "created, received, maintained, or transmitted" in electronic form. *See* 45 C.F.R. § 160.103.

89. HIPAA also protects against revealing an individual's status as a patient of a healthcare provider.²³

90. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1).

91. Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

92. Defendants unlawfully revealed Plaintiff's and Class Members' patient status to Facebook and likely other unauthorized third parties in violation of HIPAA when the Meta Pixels captured and disclosed Plaintiff's and Class Members' activity on patient-dedicated webpages of the Website, such as Patient Financial Services, Patient Education Resources, Schedule an Appointment, and the Patient Portal.

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

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes,***

²³ *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last May 14, 2024).

*without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.*²⁴

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

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

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

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

95. In addition, the Office for Civil Rights at HHS' Bulletin expressly provides that **"[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."**²⁵

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

Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (e.g. health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these

²⁴ *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (emphasis added) (updated March 18, 2024) (last visited May 4, 2024).

²⁵ *Id.*

circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.²⁶

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

How do the HIPAA Rules apply to regulated entities' use of tracking technologies?

Some regulated entities may be disclosing a variety of information to tracking technology vendors through tracking technologies placed on the regulated entity's website or mobile app, such as information that the individual types or selects when they use regulated entities' websites or mobile apps. The information disclosed might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, device IDs, or any unique identifying code.

IIHI collected on a regulated entity's website or mobile app generally is PHI, **even if the individual does not have an existing relationship with the regulated entity** and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.²⁷

²⁶ *Id.*

²⁷ *Id.* (emphasis added).

98. HIPAA applies to Defendants' webpages with tracking technologies even outside the patient portal:

Tracking on unauthenticated webpages

Regulated entities may also have unauthenticated webpages, which are webpages that do not require users to log in before they are able to access the webpage, such as a webpage with general information about the regulated entity like their location, visiting hours, employment opportunities, or their policies and procedures... **in some cases, tracking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to the tracking technology vendors.** Regulated entities are required to "[e]nsure the confidentiality, integrity, and availability of all electronic PHI the [regulated entity] creates, receives, maintains, or transmits." Thus, regulated entities that are considering the use of online tracking technologies should consider whether any PHI will be transmitted to a tracking technology vendor, and take appropriate steps consistent with the HIPAA Rules.²⁸

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

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

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

Tracking on user-authenticated webpages

²⁸ *Id.* (emphasis added).

Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. **Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to only use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.²⁹

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

102. The Bulletin notes that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," then explains how online tracking technologies violate the same HIPAA rules that have existed for decades.³⁰

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

²⁹ *Id.* (emphasis added).

³⁰ *Id.* (citing, e.g., Modifications of the HIPAA [Rules], Final Rule," 78 FR 5566, 5598, a rulemaking notice from January 25, 2013, which stated: "[P]rotected health information ... may not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a covered entity, then it is protected health information by definition since it is indicative that the individual received health care services or benefits from the covered entity, and therefore it must be protected ... in accordance with the HIPAA rules." at n. 22).

104. As a result, a healthcare provider like Defendants may not disclose PHI to a tracking technology vendor, like Meta, unless it has properly notified its Website Users and entered into a business associate agreement with the vendor in question.

105. Defendants disclosed Plaintiff's and Class Members' PHI without their consent and without a business associate agreement with Meta.

C. Defendants Transmitted a Broad Spectrum of Plaintiff's & Class Members' Identifiable Health Information to Meta via the Meta Tracking Tools.

106. Defendants' Pixel, embedded in its JavaScript Source Code on the Website, manipulates a User's browser by secretly instructing it to duplicate a User's communications (HTTP Requests) and sending those communications to Facebook.

107. This occurs because the Pixel is programmed to automatically track and transmit Users' communications, and this occurs contemporaneously, invisibly, and without the Users' knowledge.

108. Defendants' Source Code essentially commands a patient's browser to re-direct their actions on the Website (characterized as "Event Data" by the Pixel), which contain PHI, through the HTTPS protocol to Meta at a Meta "endpoint," i.e., a URL at a domain controlled by Meta that exists for the purpose of acquiring such information.

109. The information Defendants sends to Meta from its use of the Meta Pixel and other tracking tools includes, but is not limited to, the following:

- a. The exact search terms entered by a User on the Website, including searches for the User's medical symptoms and conditions, specific medical providers and their specialty, and treatments sought;
- b. descriptive URLs that describe the categories of the Website, categories that describe the current section of the Website, and the referrer URL that caused navigation to the current page;

- c. the communications a User exchanges through Defendants' Website by clicking and viewing webpages, including communications about providers and specialists, conditions, and treatments, along with the timing of those communications, including, upon information and good faith belief, whether they are made while a User is still logged in to the Patient Portal or around the same time that the User has scheduled an appointment, called the medical provider, or logged in or out of the Patient Portal;
- d. when a User sets up or schedules an appointment;
- e. when a User clicks a button to call the provider from a mobile device directly from Defendants' Website;
- f. when a User clicks to register for the Patient Portal, clicks to log into the Portal, and/or accesses other patient-dedicated web pages; and

110. Thus, Defendants are, in essence, handing patients a tapped device and once one of its webpages is loaded into the User's browser, the software-based wiretap is quietly waiting for private communications on the webpage to trigger the tap, which intercepts those communications—intended only for Defendant—and transmits those communications to unauthorized third parties such as Facebook.

111. For example, when a patient visits <https://www.uvmhealth.org/> and enters “heart disease,” “diabetes” or “stroke rehabilitation” into the search bar, their browser automatically sends an HTTP request to Defendants' web server. Defendants' web server automatically returns an HTTP response, which loads the Markup for that particular webpage.

112. The patient visiting this particular web page only sees the Markup, not the Defendants' source code or underlying HTTP Requests and Responses.

113. In reality, Defendants' Source Code and underlying HTTP Requests and Responses share the patient's personal information with Facebook, including the fact that a User was looking

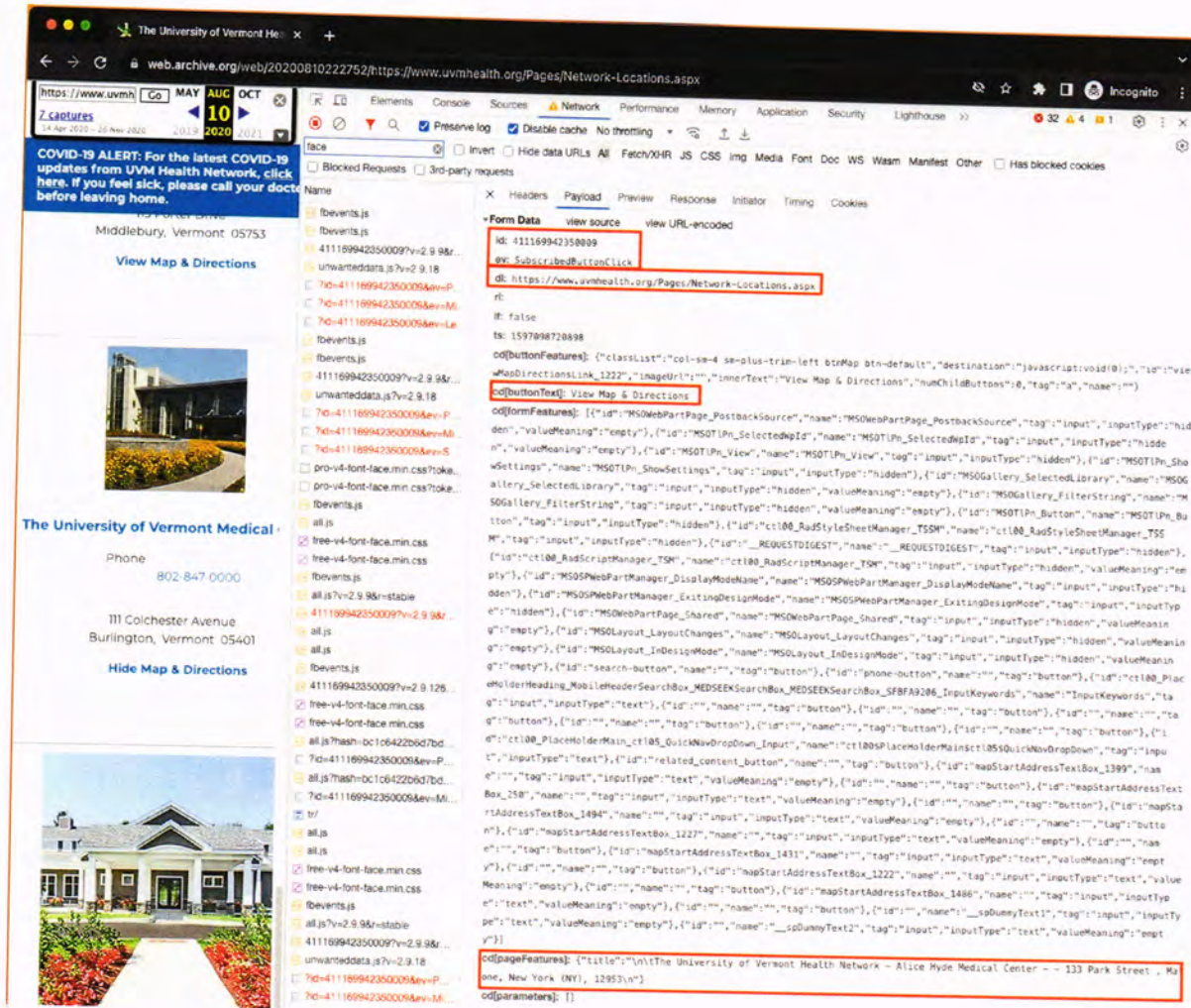
for doctors to assist with their heart disease, diabetes, or stroke diagnosis — along with the User's unique personal identifiers.

114. UVM also shares a user's activities related to finding UVM's locations through SubscribedButtonClick, PageView, and Microdata events. The image immediately below also shows the use of the Advanced Matching Parameters.

The screenshot shows the University of Vermont Health Network website. The browser's developer tools are open, displaying the Network tab. The 'Form Data' section of the selected request is visible, showing various parameters including 'id', 'ev', 'url', and 'cd(buttonText)'. The 'cd(buttonText)' parameter is highlighted with a red box, showing the value 'Locations'. The 'url' parameter is also highlighted with a red box, showing the full URL to the 'Doctors.aspx' page.

115. When a user clicks to call a UVM location and/or clicks to open UVM's Medical Center Maps & Directions, UVM sends both a Lead event and a SubscribedButtonClick event.

Again, Advanced Matching Parameters are enabled:

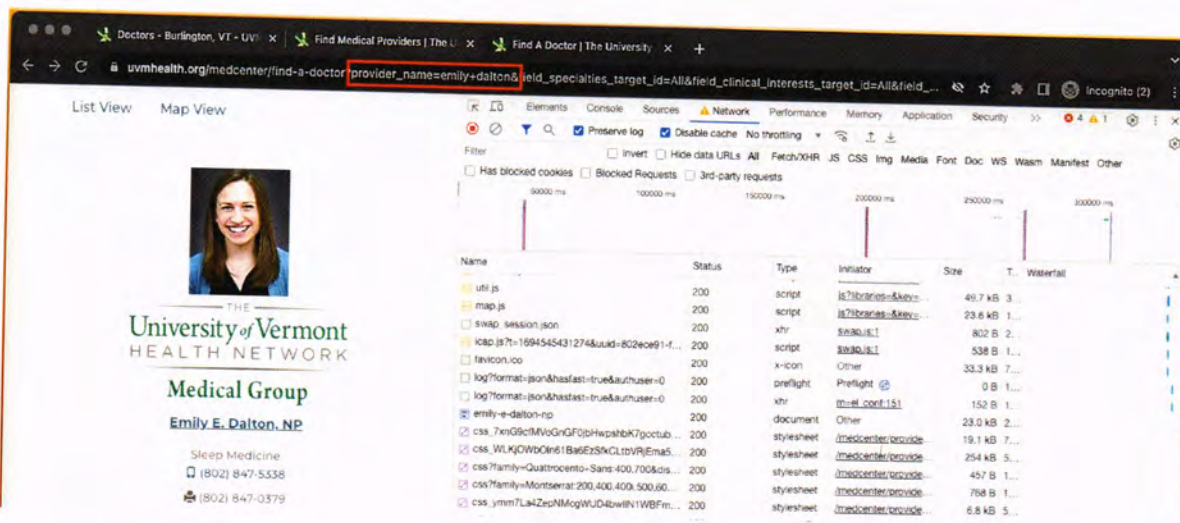


116. Defendants also discloses users' search terms as URLs are sent via the "ri" and "dl" parameters in Meta Pixel events.³¹

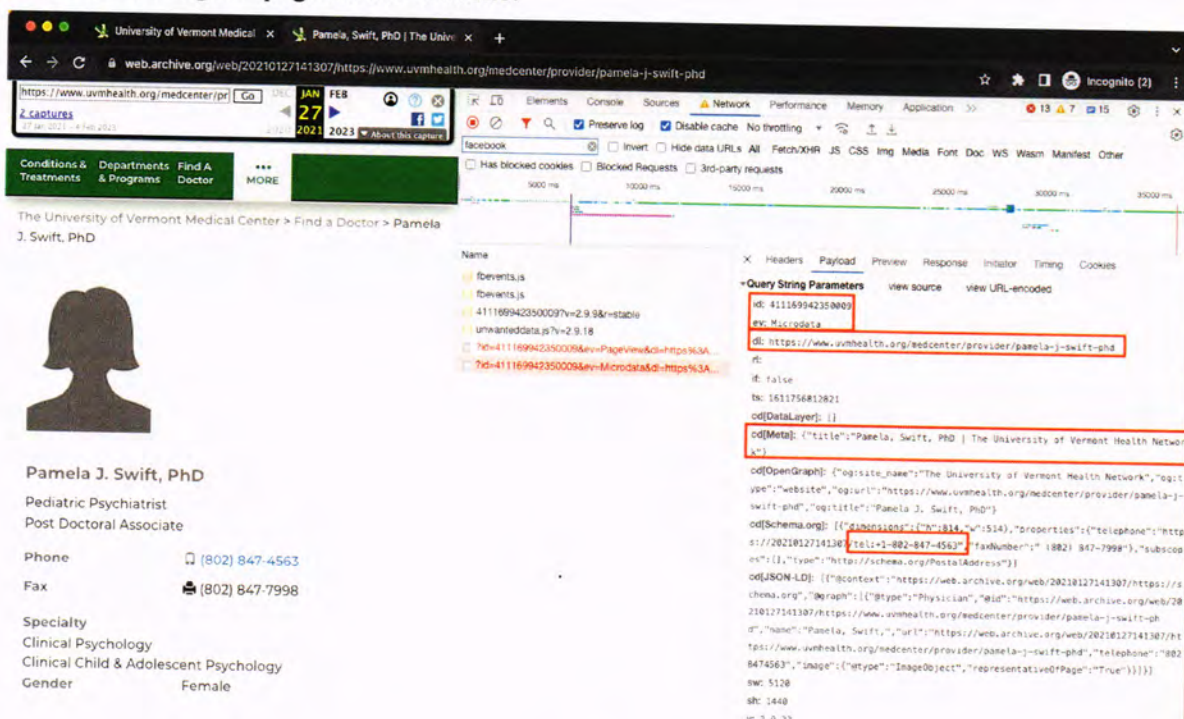
117. When a user searches for a specific practitioner, for example Emily Dalton, a sleep

³¹ A URL is the web address that your type in the address bar at the top of the screen or which appear in the address bar when you click on a link. It stands for Uniform Resource Locator. When you go to use google, the URL that appears is google.com. And when you click on google maps, the URL changes to google.com/maps. It is that extension to the URL, "maps" that provides additional pageview information that allows pixels and trackers to know more about your internet usage.

specialist, the search is disclosed with the provider's name as "Emily+Dalton".



118. In addition, UVM also sends information to Meta as a user views a specific provider's page. For example, a user's view of the page for Pamela J. Swift, a pediatric psychologist, triggered UVM's Pixel to send Microdata and PageView events revealing that the user is viewing her page on the Website.



119. The Microdata event in the image above discloses the phone number the user viewed on the physician's page.

The screenshot shows a web browser window displaying the profile of Pamela J. Swift, PhD, a Pediatric Psychiatrist and Post Doctoral Associate at the University of Vermont Medical Center. The page includes her name, title, and contact information: Phone (802) 847-4563 and Fax (802) 847-7998. Her specialties are Clinical Psychology and Clinical Child & Adolescent Psychology.

Overlaid on the page is a network inspector tool. The 'Query String Parameters' tab is selected, showing a list of parameters. The 'id' parameter is highlighted with a red box, and its value is 'https://www.uvmhealth.org/medcenter/provider/pamela-j-swift-phd'. The 'event' parameter is also highlighted, with a value of 'PageView'. The 'microdata' parameter is visible, with a value of 'https://www.uvmhealth.org/medcenter/provider/pamela-j-swift-phd'.

120. When the user interacts with links on Pamela J. Swift's page by clicking to call a phone number or to view directions, UVM sends a "Lead" event and "SubscribedButtonClick" event revealing that the user viewed and clicked on this provider's contact information.

University of Vermont Medical x Pamela, Swift, PhD | The Univ... x

web.archive.org/web/20210127141307/https://www.uvmhealth.org/medcenter/provider/pamela-j-swift-phd

https://www.uvmhealth.org/medcenter/pr... 27 JAN FEB 2021 2023 About this capture

Conditions & Treatments Departments & Programs Find A Doctor MORE

The University of Vermont Medical Center > Find a Doctor > Pamela J. Swift, PhD

Pamela J. Swift, PhD
 Pediatric Psychiatrist
 Post Doctoral Associate

Phone (802) 847-4563
 Fax (802) 847-7998

Specialty
 Clinical Psychology
 Clinical Child & Adolescent Psychology
 Gender Female

Network Inspector:

- Name: fbevents.js
- 411169942350009?v=2.9.9&n=stable
- unwanteddata.js?v=2.9.18
- Tid=411169942350008&ev=PageView&id=https%3A...
- Tid=411169942350008&ev=Microdata&id=https%3A...
- Tid=411169942350008&ev=Lead&id=https%3A%2F...
- fbevents.js
- fbevents.js
- 411169942350009?v=2.9.9&n=stable
- unwanteddata.js?v=2.9.18
- Tid=411169942350008&ev=PageView&id=https%3A...
- Tid=411169942350008&ev=Microdata&id=https%3A...

Query String Parameters:

- id: 411169942350009
- ev: Lead
- id: https://www.uvmhealth.org/medcenter/provider/pamela-j-swift-phd
- fb: 1611756837618
- cd(content.name): ClickToCallClicks
- cd(content.category): Clicks
- sw: 5120
- sh: 1440
- v: 2.9.33
- r: stable
- ec: 2
- o: 30
- fbp: fb.1.1694527858395.138449389
- fb: 1611756799087
- ooc: false
- rqm: GET

University of Vermont Medical x Pamela, Swift, PhD | The Univ... x

web.archive.org/web/20210127141307/https://www.uvmhealth.org/medcenter/provider/pamela-j-swift-phd

https://www.uvmhealth.org/medcenter/pr... 27 JAN FEB 2021 2023 About this capture

Conditions & Treatments Departments & Programs Find A Doctor MORE

The University of Vermont Medical Center > Find a Doctor > Pamela J. Swift, PhD

Pamela J. Swift, PhD
 Pediatric Psychiatrist
 Post Doctoral Associate

Phone (802) 847-4563
 Fax (802) 847-7998

Specialty
 Clinical Psychology
 Clinical Child & Adolescent Psychology
 Gender Female

Network Inspector:

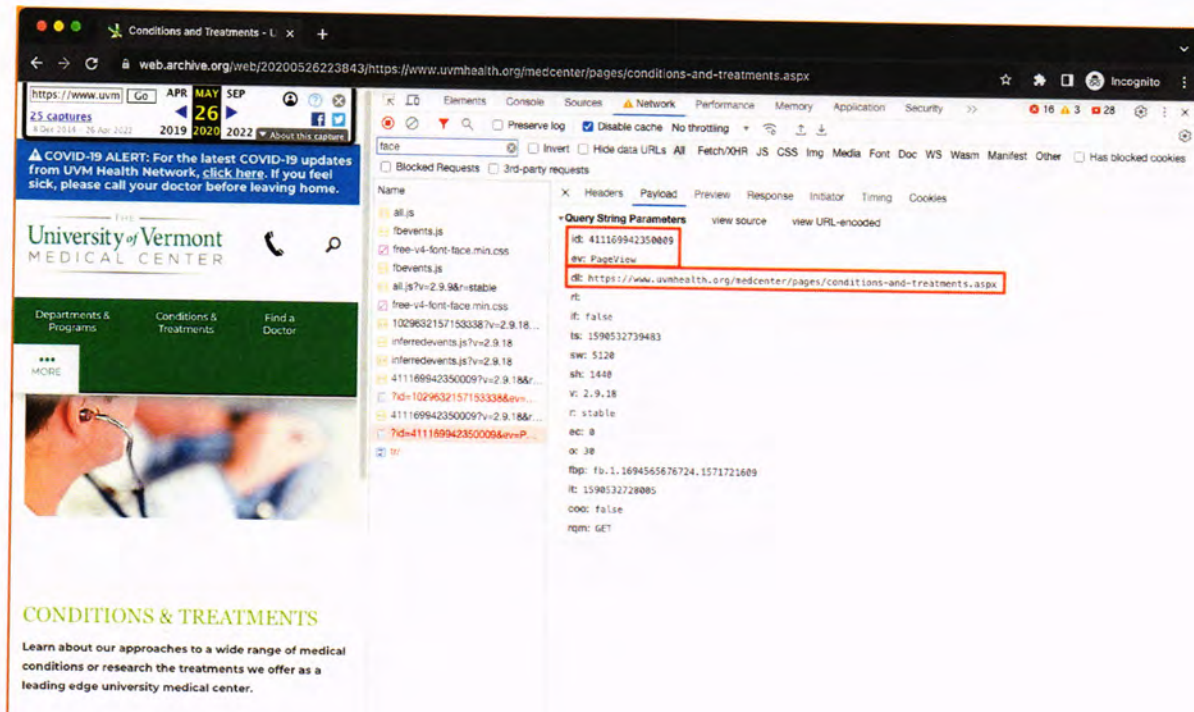
- Name: fbevents.js
- fbevents.js
- 411169942350009?v=2.9.9&n=stable
- unwanteddata.js?v=2.9.18
- Tid=411169942350008&ev=PageView&id=https%3A...
- Tid=411169942350008&ev=Microdata&id=https%3A...
- Tid=411169942350008&ev=Lead&id=https%3A%2F...
- fbevents.js
- fbevents.js
- 411169942350009?v=2.9.9&n=stable
- unwanteddata.js?v=2.9.18
- Tid=411169942350008&ev=PageView&id=https%3A...
- Tid=411169942350008&ev=Microdata&id=https%3A...
- Tid=411169942350008&ev=SubscribedButtonClick&id=https%3A%2F...

Query String Parameters:

- id: 411169942350009
- ev: SubscribedButtonClick
- id: https://www.uvmhealth.org/medcenter/provider/pamela-j-swift-phd
- fb: 1611756863005
- cd(buttonFeatures): {"classList": "btn btn-primary pull-left", "destination": "https://www.google.com/maps/dir/..."}
- cd(buttonText): Directions
- cd(formFeatures): {}
- cd(pageFeatures): {"title": "Pamela, Swift, PhD | The University of Vermont Medical Center"}
- cd(parameters): {}
- sw: 5120
- sh: 1440
- v: 2.9.33
- r: stable
- ec: 2
- o: 30
- fbp: fb.1.1694527858395.138449389
- fb: 1611756796789

121. UVM continues its disclosures as users view content about conditions treated by and treatments offered by UVM.

122. For instance, UVM sends PageView events upon a user's launch of the Conditions & Treatments page, and, for example, the sleep apnea page and the page for UVM's sleep center.



The screenshot shows a web browser window displaying the University of Vermont Medical Center website. The address bar shows the URL: <https://www.uvmhealth.org/medcenter/pages/conditions-and-treatments.aspx>. A network inspector is open on the right side of the browser, showing the 'Query String Parameters' for a request to the same URL. The parameters include:

- id: 1829632157153338
- pv: PageView
- dt: https://www.uvmhealth.org/medcenter/pages/conditions-and-treatments.aspx
- rt:
- ft: false
- tn: 1598532757986
- sw: 5120
- sh: 1440
- vt: 2.9.18
- r: stable
- ec: 0
- o: 28
- fb: fb-1,1694527858395,138449389
- lt: 1598532756462
- oex: false
- qgm: GET

The website content includes a header with the University of Vermont Medical Center logo and navigation links. A main section titled 'CONDITIONS & TREATMENTS' is visible, with a sub-header 'Learn about our approaches to a wide range of medical conditions or research the treatments we offer as a leading edge university medical center.'

The screenshot shows a web browser window displaying the University of Vermont Medical Center website. The address bar shows the URL: <https://www.uvmhealth.org/medcenter/Pages/Conditions-and-Treatments/Sleep-Apnea.aspx>. A network inspector is open on the right side of the browser, showing the 'Query String Parameters' for a request to the same URL. The parameters include:

- id: 411169942350009
- pv: PageView
- dt: https://www.uvmhealth.org/medcenter/Pages/Conditions-and-Treatments/Sleep-Apnea.aspx
- rt:
- ft: false
- tn: 1467246804797
- vt: 2.5.0
- pv: visible

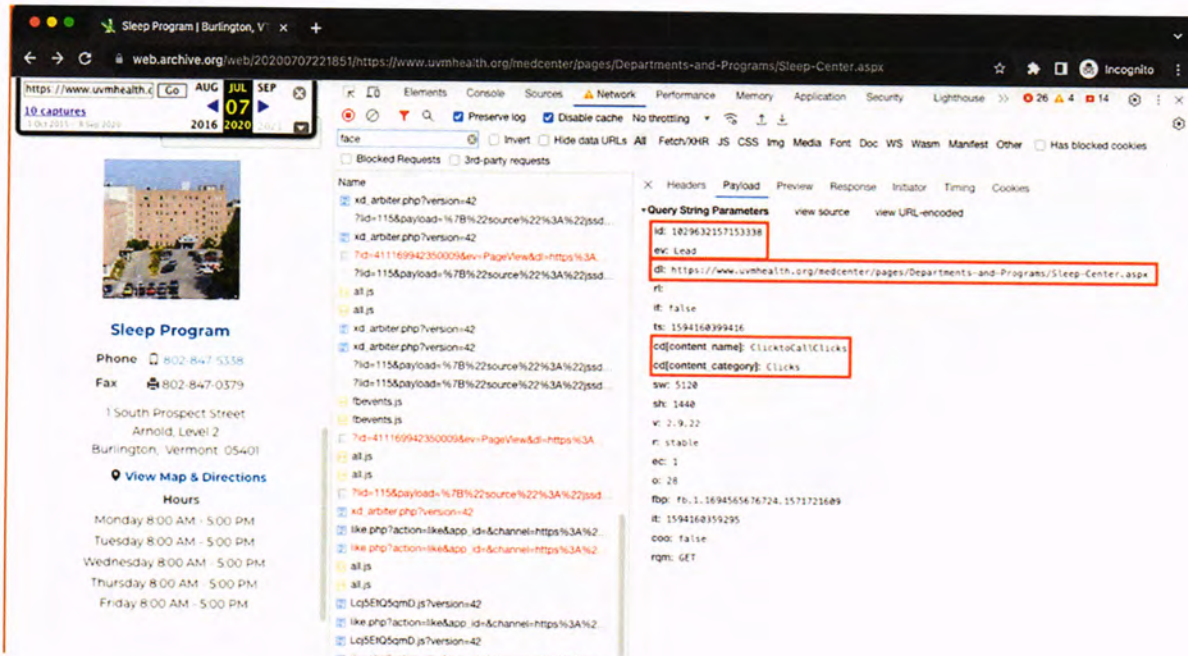
The website content includes a header with the University of Vermont Medical Center logo and navigation links. A main section titled 'Sleep Apnea: What You Need to Know' is visible, with a sub-header 'The Sleep Center at The University of Vermont Medical Center in Burlington, VT provides expert diagnosis and comprehensive care for sleep apnea.'

123. UVM also sends a companion Microdata event with the PageView event when the user launches the Conditions & Treatments page which reveals to Meta the page the user is viewing the contents of that page.

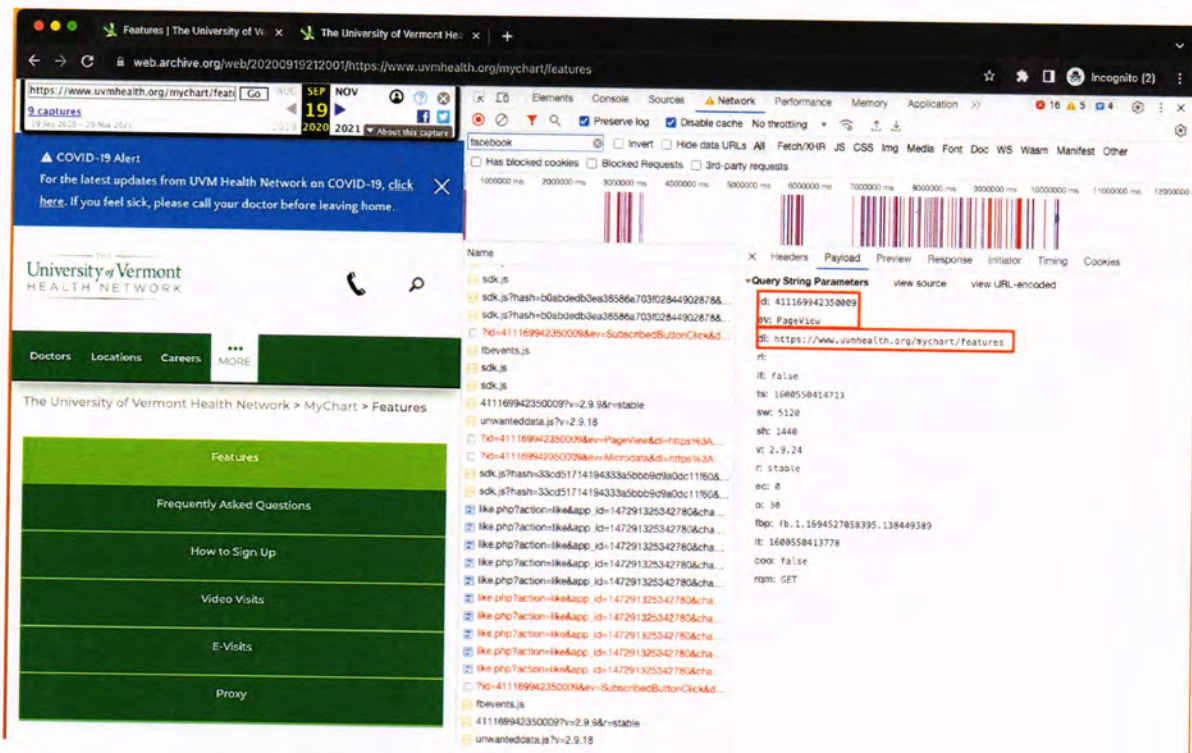
The screenshot shows a web browser displaying the University of Vermont Medical Center's "Conditions & Treatments" page. The browser's developer tools are open, showing the Network tab. A request named "face" is selected, and the "Form Data" sub-tab is active. The "Form Data" table shows the following data:

Field	Value
id	411169942350009
ev	Microdata
url	https://www.uvmhealth.org/medcenter/pages/conditions-and-treatments.aspx
dt	false
ts	1508532739989
cd[DataLayer]	[]
cd[Meta]	{ "title": "Conditions and Treatments - University of Vermont Medical Center - Burlington, VT", "description": "Learn about our approaches to a wide range of medical conditions or research the treatments we offer as a leading edge university medical center." }
cd[OpenGraph]	{ "og:title": "Conditions and Treatments - University of Vermont Medical Center - Burlington, VT", "og:site_name": "Burlington, VT - University of Vermont Medical Center", "og:url": "https://www.uvmhealth.org/medcenter/pages/conditions-and-treatments.aspx", "og:description": "Learn about our approaches to a wide range of medical conditions or research the treatments we offer as a leading edge university medical center." }
cd[Schema.org]	{ "@context": "https://web.archive.org/web/20200526223843/http://schema.org", "@type": "Organization", "url": "https://web.archive.org/web/20200526223843/https://www.uvmhealth.org/medcenter", "contactPoint": { "@type": "ContactPoint", "telephone": "+1-802-847-8000", "contactType": "customer service" } }, "@context": "https://web.archive.org/web/20200526223843/http://schema.org", "@type": "Organization", "name": "The University of Vermont Medical Center", "url": "https://web.archive.org/web/20200526223843/https://www.uvmhealth.org/medcenter", "sameAs": ["https://web.archive.org/web/20200526223843/https://www.facebook.com/TheUniversityofVermontMedicalCenter", "https://web.archive.org/web/20200526223843/https://twitter.com/uvmmedcenter", "https://web.archive.org/web/20200526223843/https://plus.google.com/b/103622620971804487071/103622620971804487071/about", "https://web.archive.org/web/20200526223843/http://instagram.com/uvmmedcenter", "https://web.archive.org/web/20200526223843/http://www.youtube.com/c/TheUniversityofVermontMedicalCenter", "https://web.archive.org/web/20200526223843/http://www.linkedin.com/company/university-of-vermont-medical-center"] }

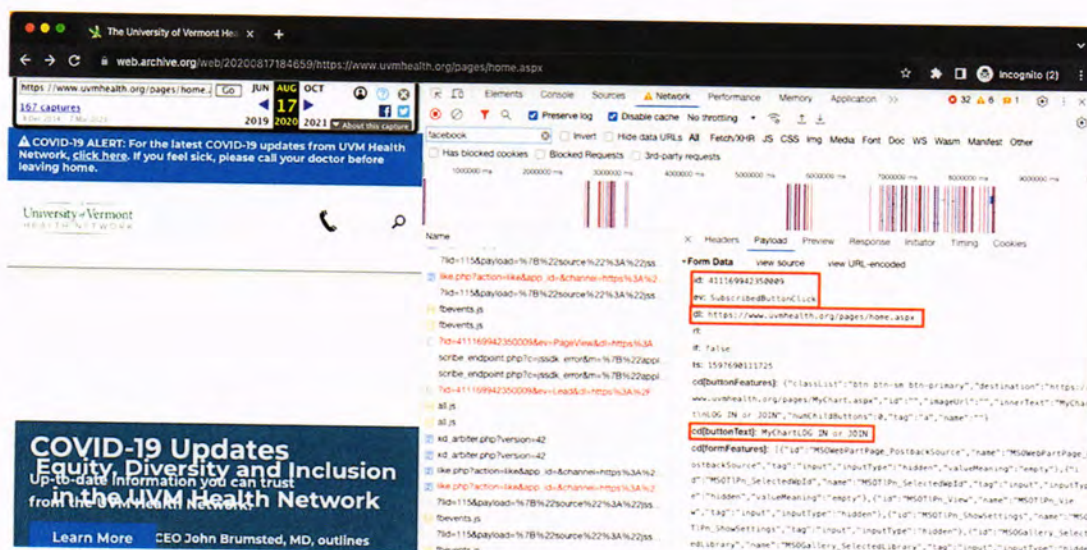
124. When the user clicks to call from the UVM sleep center page, Defendants send a Lead event to Meta notifying them of the user's action.



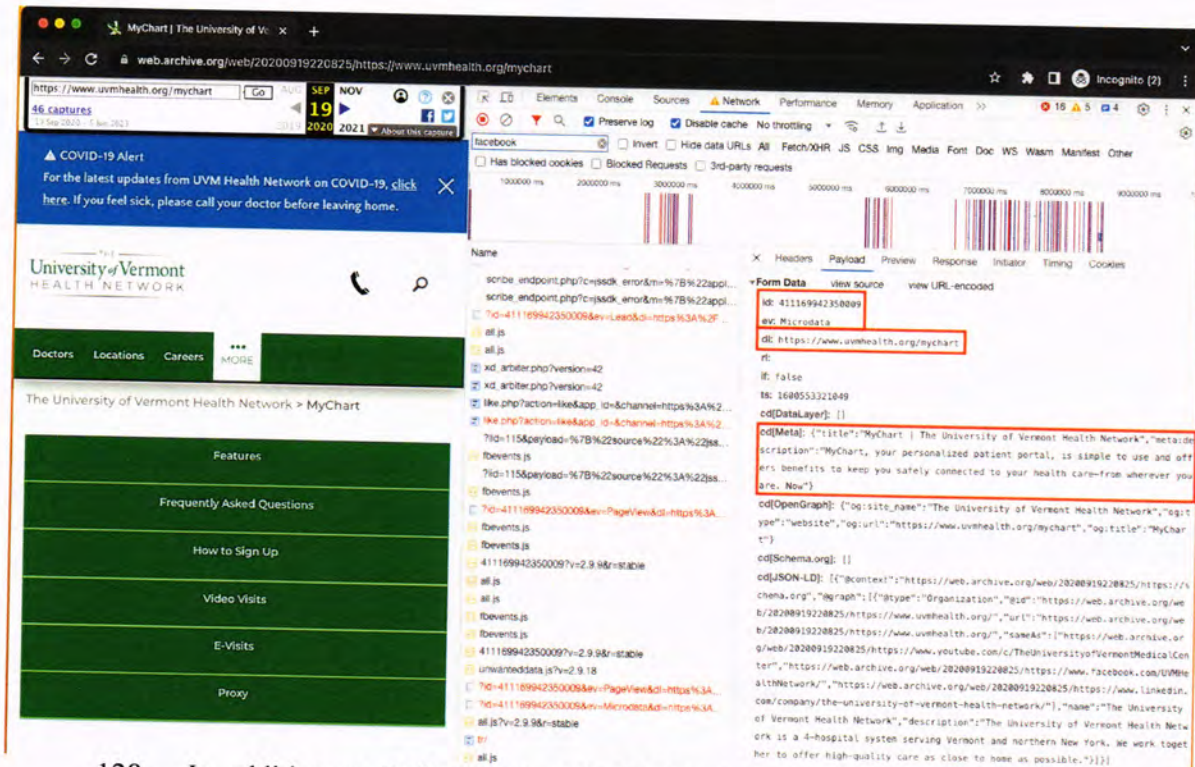




126. Once the user is on the main UVM MyChart landing page, the user's interactions, such as clicks to sign up, learn more about MyChart, and use of an activation code, each trigger a SubscribedButtonClick event notifying Meta of the user's actions.



127. Once the user launches the page to use the activation code to access MyChart, UVM also sends PageView and Microdata events notifying Meta which page the user is viewing and the contents of that page.



128. In addition to Defendants' main MyChart landing page, Defendants also had MyChart landing pages for each individual location. This analysis uses the UVM Medical Center in Burlington, Vermont as a representation of UVM's disclosures of user activities on the individualized MyChart landing pages.

129. When a user clicked to login to or to create an account with the UVM Medical Center MyChart, UVM sent SubscribedButtonClick events for each event.

130. From the analysis above and information gathered by Plaintiff's counsel, it is clear that extensive tracking was in place on the UVM site from at least July of 2016 to spring of 2022.

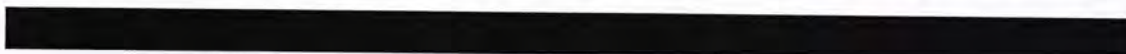
131. Immediately upon a User's arrival on Defendants' homepage, Defendants

immediately sent a pair of PageView and Microdata events to Facebook revealing that the User was on the homepage.

132. As Users navigated beyond the homepage, Defendants continued to disclose User data including Users': (i) keyword search activities; (ii) appointment activities; (iii) medical conditions and treatment sought; and (iv) MyChart login activities, at the very least.

133. In recent months, following a wave of negative press and litigation against other healthcare companies for the same unlawful activities, Defendants have removed the Meta Pixel from its Website and has re-configured its source code.

134. However, because of the way Defendants' source code operated with the embedded Meta Pixel, when Plaintiff used the search bar on the Website to look for medical treatments for

 were transmitted by Defendants' Pixel to Meta, disclosing his specific medical conditions.

135. When Plaintiff and Class Members clicked on Defendants' "Medical Services" tab, it took them to the list of services offered by Defendants to Users in need of various medical treatments. On those pages the User can further narrow their search results by services offered by Defendant.

136. The User's selections and filters are transmitted to Facebook via the Meta Pixels, even if they contain the User's treatment, procedures, medical conditions, or related queries, without alerting the User, and the images above confirm that the communications Defendants sends to Facebook contain the User's Private Information and personal identifiers, including but not limited to their IP address, Facebook ID, and datr and fr cookies, along with the search filters the User selected.

137. For example, a diabetes patient in search for diabetes services can search for various diabetes treatment options and information, from “endocrinology clinic” and “diabetes prevention” to resources intended to help patients.³²

138. From the moment the patient begins searching for diabetes treatment their selections or search parameters are automatically transmitted by the Pixel to Facebook along with the User’s unique personal identifiers.

139. The transmission identifies the User as a patient: (i) seeking medical care from Defendants via the Website; (ii) who has diabetes; and (iii) who is searching for diabetes services.

140. Similarly, a patient who has experienced a stroke can search for post-stroke treatments, including rehabilitation services.

141. From the moment the patient begins searching for post-stroke treatment their selections or search parameters are automatically transmitted by the Pixel to Facebook along with the User’s unique personal identifiers.

142. The transmission identifies the User as a patient: (i) seeking medical care from Defendants via the Website; (ii) who has had a stroke; and (iii) who is searching for stroke rehabilitation services.

143. If the patient chooses to click the phone number for a specific provider, that action is shared with Meta as well, via a “SubscribedButtonClick” event which captures the phone number of the provider accessed by the patient.

³² See *Diabetes Care at the UVM Medical Center*, UVM Health <https://www.uvmhealth.org/medcenter/departments-and-programs/diabetes>.

144. As described above, if the patient selects other services, those search parameters are also automatically transmitted to Facebook by Defendants' Pixel, along with the patient's personal identifiers.

145. For example, after Plaintiff's [REDACTED], he looked up information and appointments through Defendants' website.

146. This information would have been disclosed to Facebook (and likely other unauthorized third parties at least in the form of a descriptive URL, [REDACTED], along with Plaintiff's unique personal identifiers including his Facebook ID and IP address.

147. For Plaintiff, Defendants would have disclosed that starting in early 2021 he was looking up [REDACTED], including but not limited to sharing the descriptive URLs that she visited on Defendants' Website.

D. Defendants' Website Sent Plaintiff's and Class Members' PHI to Facebook Together with their Unique Personal Identifiers.

148. As described herein, Defendants' Meta Pixel (and other third-party trackers) sent sensitive Private Information to Facebook, including but not limited to Plaintiff's and Class Members': (i) status as medical patients; (ii) health conditions; (iii) sought treatments or therapies; (iv) exact terms and phrases entered into Defendants' search bar; (v) sought providers and their specialties; (vi) selected locations or facilities for treatment and (vii) web pages viewed.

149. Importantly, the Private Information Defendants' Pixel sent to Facebook was sent alongside Plaintiff's and Class Members' personal identifiers, including patients' IP address and cookie values such as their unique Facebook ID, thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts.

150. Through the source code deployed by Defendant, the cookies that it uses to help Facebook identify patients include but are not necessarily limited to cookies named: “c_user,” “datr,” “fr,” and “fbp.”

151. A User’s FID is linked to their Facebook profile, which generally contains a wide range of demographics and other information about the User, including pictures, personal interests, work history, relationship status, and other details. Because the User’s Facebook Profile ID uniquely identifies an individual’s Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the User’s corresponding Facebook profile.

152. The “datr” cookie identifies the patient’s specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient’s specific web browser and is therefore a means of identification for Facebook users.

153. The “fr” cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.³³ Facebook, at a minimum, uses the fr cookie to identify Users.³⁴

154. At each stage, Defendants also utilized the _fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a User:³⁵

³³ See Gunes Acar et al., *Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission* 16 (March 27, 2015), https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.

³⁴ *Cookies Policy*, META, <https://www.facebook.com/policy/cookies/> (last May 14, 2024).

³⁵ *Id.*

155. The fr cookie expires after ninety (90) days unless the User's browser logs back into Facebook.³⁶ If that happens, the time resets, and another ninety (90) days begins to accrue.

156. The _fbp cookie expires after ninety (90) days unless the User's browser accesses the same website.³⁷ If that happens, the time resets, and another ninety (90) days begins to accrue.

157. The Facebook Meta Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—i.e., Defendant.³⁸

158. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook.³⁹

159. The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

160. Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link to FIDs and corresponding Facebook profiles.

161. As shown in the figures above, Defendants sent these identifiers with the event data.

162. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendants to disclose their Private Information, nor did they authorize any assistance with intercepting their communications.

³⁶ *Id.*

³⁷ *Id.*

³⁸ This is confirmable by using developer tools to inspect a website's cookies and track network activity.

³⁹ This is confirmable by tracking network activity.

163. Plaintiff was never provided with any written notice that Defendants disclosed its Website Users' Private Information nor were they provided any means of opting out of such disclosures.

164. Despite this, Defendants knowingly and intentionally disclosed Plaintiff's Private Information to Facebook.

E. Defendants Violates Its Promises to Users and Patients to Protect Their Confidentiality.

165. Beyond Defendants' legal obligations to protect the confidentiality of individuals' Private Information, Defendants' privacy policies and online representations affirmatively and unequivocally state that any personal information provided to Defendants will remain secure and protected.⁴⁰

166. Further, Defendants represents to Users that it will only disclose Private Information provided to them under certain circumstances, none of which apply here.⁴¹ Defendants' privacy policies do not permit Defendants to use and disclose Plaintiff's and Class Members' Private Information for marketing purposes.

167. In fact, Defendants acknowledges in its Notice of Privacy Practices that "we do not sell any personal information."⁴²

⁴⁰ *The University of Vermont Health Network Web Site Privacy Policy*, UNIVERSITY OF VERMONT HEALTH, <https://web.archive.org/web/20170428064038/https://www.uvmhealth.org/pages/privacy-policy.aspx> (last visited May 14, 2024).

⁴¹ *See id.*

⁴² *See id.*

168. Moreover, Defendants represents that it will only collect PHI “if you choose to provide it to us.”⁴³

169. Further, Defendants’ Privacy Policy represents: “We do use cookies, but only to determine whether someone has previously visited the Web site.”⁴⁴

170. Defendants failed to issue a notice that Plaintiff’s and Class Members’ Private Information had been impermissibly disclosed to an unauthorized third party. In fact, Defendants never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications, data, and Private Information with Meta and other unauthorized third parties.⁴⁵

171. Through Plaintiff’s payment for healthcare services with Defendants for many years, the terms of Defendants’ privacy policies necessarily formed essential terms of its contracts for those services. Plaintiff understood that as part of their bargain for healthcare services with Defendant, Defendants would keep their promises of confidentiality regarding their sensitive PHI, however it was to be received by Defendant.

172. Defendants has unequivocally failed to adhere to their promise to safeguard Private Information of its Users. Defendants has made these privacy policies and commitments available

⁴³ See *id.*

⁴⁴ See *id.*

⁴⁵ In contrast to Defendant, medical providers which have installed the Meta Pixel on their websites have provided its patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. See, e.g., *Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf; Annie Burky, *Advocate Aurora says 3M patients’ health data possibly exposed through tracking technologies*, FIERCE HEALTHCARE (October 20, 2022), <https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3>; *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWswire (August 19, 2022), <https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html>.

on its websites. Defendants includes these privacy policies and commitments to maintain the confidentiality of its Users' sensitive information as terms of its contracts with those Users, including contracts entered with Plaintiff and the Class Members. In these contract terms and other representations to Plaintiff and Class Members and the public, Defendants promised to take specific measures to protect Plaintiff's and Class Members' Private Information, consistent with industry standards and independent from federal and state law. However, it failed to do so.

173. Even non-Facebook users can be individually identified via the information gathered on the Digital Platforms, like an IP address or personal device identifying information. This is precisely the type of information for which HIPAA requires the use of de-identification techniques to protect patient privacy.⁴⁶

174. In fact, in an action currently pending against Facebook related to use of its Pixel on healthcare provider Website, Facebook explicitly stated it requires Pixel users to "post a prominent notice on every page where the Pixel is embedded and to link from that notice to information about exactly how the Pixel works and what is being collected through it, so it is not invisible."⁴⁷ Defendants did not post such a notice.

175. Facebook further stated that "most providers [...] will not be sending [patient information] to Meta because it violates Meta's contracts for them to be doing that."⁴⁸

⁴⁶ *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule*, *supra*, note 27.

⁴⁷ See Transcript of the argument on Plaintiff's Motion for Preliminary Injunction in *In re Meta Pixel Healthcare Litig.*, Case No. CV-22-03580-WHO (N.D. Cal. Nov. 9, 2022) (Hon. J. Orrick), at 19:12-18; see also *In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218 (N.D. Cal. Dec 22, 2022).

⁴⁸ *Id.* at 7:20-8:11.

176. Despite a lack of disclosure, Defendants allowed third parties to “listen in” on patients’ confidential communications and to intercept and use for advertising purposes the very information they promised to keep private, in order to bolster their profits.

F. Plaintiff and Class Members Reasonably Believed That Their Confidential Medical Information Would Not Be Shared with Third Parties.

177. Plaintiff and Class Members were aware of Defendants’ duty of confidentiality when they sought medical services from Defendant.

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

179. Personal data privacy and obtaining consent to share Private Information are material to Plaintiff and Class Members.

180. Plaintiff and Class Members relied to their detriment on Defendants’ uniform representations and omissions regarding protection privacy, limited uses, and lack of sharing of their Private Information.

181. Now that their sensitive personal and medical information is in possession of third parties, Plaintiff and Class Members face a constant threat of continued harm including bombardment of targeted advertisements based on the unauthorized disclosure of their personal data. Collection and sharing of such sensitive information without consent or notice poses a great threat to individuals by subjecting them to the never-ending threat of identity theft, fraud, phishing scams, and harassment.

G. Plaintiff and Class Members Have No Way of Determining Widespread Usage of Invisible Pixels.

182. Plaintiff and Class Members did not realize that tracking Pixels exist because they are invisibly embedded within Defendants' web pages that Users might interact with.⁴⁹ Patients and Users of Defendants' Website do not receive any alerts during their uses of Defendants' Website stating that Defendants tracks and shares sensitive medical data with Facebook, allowing Facebook and other third parties to subsequently target all Users of Defendants' website for marketing purposes.

183. Plaintiff and Class Members trusted Defendants' Website when inputting sensitive and valuable Private Information. Had Defendants disclosed to Plaintiff and Class Members that every click, every search, and every input of sensitive information was being tracked, recorded, collected, and disclosed to third parties, Plaintiff and Class Members would not have trusted Defendants' Website to input such sensitive information.

184. Defendants knew or should have known that Plaintiff and Class Members would reasonably rely on and trust Defendants' promises regarding the tracking privacy and uses of their Private Information. Furthermore, any person visiting a health website has a reasonable understanding that medical providers must adhere to strict confidentiality protocols and are bound not to share any medical information without their consent.

185. By collecting and sharing Users' Private Information with Facebook and other unauthorized third parties, Defendants caused harm to Plaintiff, Class Members, and all affected individuals.

⁴⁹ See, e.g., FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FED. TRADE COMM'N (March 16, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>.

186. Furthermore, once Private Information is shared with Facebook, such information may not be effectively removed, even though it includes personal and private information.

187. Plaintiff fell victim to Defendants' unlawful collection and sharing of their sensitive medical information using the Meta Pixel tracking code on Defendants' Website.

H. Defendants Knew Plaintiff's Private Information Included Sensitive Medical Information, Including Medical Records.

188. By virtue of how the Meta Pixel works, i.e., sending all interactions on a website to Facebook, Defendants were aware that their Users' Private Information would be sent to Facebook when they researched specific medical conditions and/or treatments, looked up providers, made appointments, typed specific medical queries into the search bar, and otherwise interacted with Defendants' Website.

189. At all times relevant herein Meta notified its partners, including Defendants, to have the rights to collect, use, and share user data before providing any data to Meta.⁵⁰ Although Meta's

⁵⁰ See *In re Meta Pixel Healthcare Litig.*, No. 22-cv-03580-WHO, 2022 U.S. Dist. LEXIS 230754, at *13-14 (N.D. Cal. Dec. 22, 2022).

intent is questionable, Defendants had been on notice of this Pixel-tracking ever since they activated such Pixel technology on their Website.

190. Meta changed this provision again in July 2022, while still requiring partners to have the right to share patient information with Meta.⁵¹

Information from partners.

Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities off of our Products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have an account or are logged into our Products. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.

Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. Learn more about the types of partners we receive data from.

To learn more about how we use cookies in connection with Meta Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.

How do we collect or receive this information from partners?

Partners use our Business Tools, integrations and Meta Audience Network technologies to share information with us.

These Partners collect your information when you visit their site or app or use their services, or through other businesses or organizations they work with. **We require Partners to have the right to collect, use and share your information before giving it to us.**

⁵¹ Meta, *Data Policy: Information from Partners, vendors and third parties* (Jan. 1, 2023), <https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors>.

191. Defendants had the explicit option to disable the Pixel technology on their Website, but chose not to exercise this option, thereby continuing to share data with Facebook despite the availability of preventive measures.

192. Meta advised third party entities, like Defendant, to refrain from sending any information they did not have the legal right to send and expressly emphasized not to transmit health information. Yet, Defendant, in direct contravention of these disclosures, and more importantly despite Defendants' promises to keep all health-related data about patients confidential, continued to employ Pixel tracking on its Website, thereby sharing sensitive patient data without proper authorization or consent.

I. Plaintiff and Class Members Have a Reasonable Expectation of Privacy in Their Private Information, Especially with Respect to Sensitive Medical Information.

193. Plaintiff and Class Members have a reasonable expectation of privacy in their Private Information, including personal information and sensitive medical information.

194. HIPAA sets national standards for safeguarding protected health information. For example, HIPAA limits the permissible uses of health information and prohibits the disclosure of this information without explicit authorization. See 45 C.F.R. § 164. HIPAA also requires that covered entities implement appropriate safeguards to protect this information. See 45 C.F.R. § 164.530(c)(1).

195. This federal legal framework applies to health care providers, including Defendant.

196. Given the application of HIPAA to the Defendant, Plaintiff and the members of the Class had a reasonable expectation of privacy over their PHI.

197. Several studies examining the collection and disclosure of consumers' sensitive medical information confirm that the collection and unauthorized disclosure of sensitive medical

information from millions of individuals, as Defendants have done here, violates expectations of privacy that have been established as general societal norms.

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

199. For example, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.⁵² Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.⁵³

200. Users act consistent with these preferences. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.⁵⁴

⁵² *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

⁵³ *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (November 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

⁵⁴ Margaret Taylor, *How Apple Screwed Facebook*, WIRED (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

201. Medical data is particularly even more valuable because unlike other personal information, such as credit card numbers which can be quickly changed, medical data is static. This is why companies possessing medical information, like Defendant, are intended targets of cyber-criminals.⁵⁵

202. Patients using Defendants' Website must be able to trust that the information they input including their physicians, their health conditions and courses of treatment will be protected.

203. Indeed, numerous state and federal laws require this. And these laws are especially important when protecting individuals with particular medical conditions such as HIV or AIDS that can and do subject them to regular discrimination.

204. Furthermore, millions of Americans keep their health information private because it can become the cause of ridicule and discrimination. For instance, despite the anti-discrimination laws, persons living with HIV/AIDS are routinely subject to discrimination in healthcare, employment, and housing.⁵⁶

205. The concern about sharing medical information is compounded by the reality that advertisers view this type of information as particularly high value. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born.

⁵⁵ Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS (September 24, 2014), <https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924>.

⁵⁶ Bebe J. Anderson, JD, *HIV Stigma and Discrimination Persist, Even in Health Care*, AMA J. ETHICS (December 2009), <https://journalofethics.ama-assn.org/article/hiv-stigma-and-discrimination-persist-even-health-care/2009-12>.

206. As one article put it: “the datafication of family life can begin from the moment in which a parent thinks about having a baby.”⁵⁷ The article continues, “[c]hildren today are the very first generation of citizens to be datafied from before birth, and we cannot foresee—as yet—the social and political consequences of this historical transformation. What is particularly worrying about this process of datafication of children is that companies like . . . Facebook . . . are harnessing and collecting multiple typologies of children’s data and have the potential to store a plurality of data traces under unique ID profiles.”⁵⁸

207. Other privacy law experts have expressed concerns about the disclosure to third parties of a users’ sensitive medical information. For example, Dena Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra Labs—explained that having your personal health information disseminated in ways you are unaware of could have serious repercussions, including affecting your ability to obtain life insurance and how much you pay for that coverage, increase the rate you are charged on loans, and leave you vulnerable to workplace discrimination.⁵⁹

208. Defendants surreptitiously collected and used Plaintiff’s and Class Members’ Private Information, including highly sensitive medical information, through Meta Pixel in violation of Plaintiff’s and Class Members’ privacy interests.

⁵⁷ Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, MIT PRESS READER (January 14, 2021), <https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/>.

⁵⁸ *Id.*

⁵⁹ See Class Action Complaint, *Jane Doe v. Regents of the Univ. of Cal. d/b/a UCSF Medical Center*, CLASS ACTION (Feb. 9, 2023), <https://www.classaction.org/media/doe-v-regents-of-the-university-of-california.pdf>.

J. Defendants Were Enriched & Benefitted from the Use of the Pixel & other Tracking Technologies that Enabled the Unauthorized Disclosures Alleged Herein.

209. Meta advertises its' Pixel as a piece of code "that can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting. And when you use the Conversions API alongside the Pixel, it creates a more reliable connection that helps the delivery system decrease your costs."⁶⁰

210. Retargeting is a form of online marketing that targets users with ads based on previous internet communications and interactions. Retargeting operates through code and tracking pixels placed on a website and cookies to track website visitors and then places ads on other websites the visitor goes to later.⁶¹

211. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Facebook via the tracking technologies and the Pixel embedded on, in this case, Defendants' Website.

212. Through this process, the Meta Pixel loads and captures as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Pixel captures, "includes URL names of pages visited, and actions taken - all of which could be potential examples of health information."⁶²

⁶⁰ *What is the Meta Pixel*, <https://www.facebook.com/business/tools/meta-pixel> (emphasis added) (last May 14, 2024).

⁶¹ *The complex world of healthcare retargeting*, <https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/> (last May 14, 2024).

⁶² *Id.*

213. In exchange for disclosing the Private Information of their patients, Defendants were compensated by Facebook and likely other third parties in the form of enhanced advertising services and more cost-efficient marketing on their platform.

214. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many are not HIPAA-complaint or are only HIPAA-compliant if certain steps are taken.⁶³

215. For example, Freshpaint a healthcare marketing vendor, cautioned that “Meta isn’t HIPAA-compliant”, and “If you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now.”⁶⁴

216. Medico Digital also warns that “retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences.”⁶⁵

217. Thus, utilizing the Pixels directly benefits Defendants by, among other things, reducing the cost of advertising and retargeting.

K. Plaintiff’s & Class Members’ Private Information Has Substantial Value.

218. Plaintiff’s and Class Members’ Private Information had value, and Defendants’ disclosure and interception harmed Plaintiff and the Class by not compensating them for the value of their Private Information and in turn decreasing the value of their Private Information.

⁶³ See PIWIK Pro, *The guide to HIPAA compliance in analytics*, <https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf> (explaining that Google Analytics 4 is not HIPAA-compliant) (last May 14, 2024).

⁶⁴ *Id.*

⁶⁵ *The complex world of healthcare retargeting*, *supra*, note 61.

219. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the tech economy.

220. The robust market for Internet user data has been analogized to the “oil” of the tech industry.⁶⁶ A 2015 article from TechCrunch accurately noted that “Data has become a strategic asset that allows companies to acquire or maintain a competitive edge.”⁶⁷ That article noted that the value of a single Internet user—or really, a single user’s data—varied from about \$15 to more than \$40.

221. 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.

222. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use.

223. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiff herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.⁶⁸

224. Healthcare data is particularly valuable on the black market because it often contains all of an individual’s PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

⁶⁶ See *The world’s most valuable resource is no longer oil, but data*, <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (last May 14, 2024).

⁶⁷ See <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/> (last May 14, 2024).

⁶⁸ See *10 Apps for Selling Your Data for Cash*, <https://wallethacks.com/apps-for-selling-your-data/> (last May 14, 2024).

225. In 2023, the Value Examiner published a report that focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of “such data should ensure it is priced at fair market value to mitigate any regulatory risk.”⁶⁹

226. In 2021, Trustwave Global Security published a report entitled Hackers, breaches and the value of healthcare data. With respect to healthcare data records, the report found that they may be valued at up to \$250 per record on the black market, compared to \$5.40 for the next highest value record (a payment card).⁷⁰

227. The value of health data has also been reported 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.⁷¹

228. 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.”⁷²

⁶⁹ See *Valuing Healthcare Data*, <https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf> (last May 14, 2024).

⁷⁰ See <https://www.imprivata.com/blog/healthcare-data-new-prize-hackers> (citing *The Value of Data*, https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf) (last May 14, 2024).

⁷¹ See <https://time.com/4588104/medical-data-industry/> (last May 14, 2024).

⁷² See <https://www.cnn.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last May 14, 2024).

229. The dramatic difference in the price of healthcare data when compared to other forms of private information that is commonly sold is evidence of the value of PHI.

230. But these rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

231. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

TOLLING, CONCEALMENT & ESTOPPEL

232. The applicable statutes of limitation have been tolled as a result of Defendants' knowing and active concealment and denial of the facts alleged herein.

233. Defendants secretly incorporated the Meta Pixel into its Website and patient portals, providing no indication to Users that their User Data, including their Private Information, would be disclosed to unauthorized third parties.

234. Defendants had exclusive knowledge that the Meta Pixel was incorporated on its Website, yet failed to disclose that fact to Users, or inform them that by interacting with its Website, Plaintiff's and Class Members' User Data, including Private Information, would be disclosed to third parties, including Facebook.

235. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendants' conduct because the incorporation of Meta Pixels is highly technical and there were no disclosures or other indications that would inform a reasonable consumer that Defendants was disclosing and allowing Facebook to intercept Users' Private Information.

236. The earliest Plaintiff and Class Members could have known about Defendants' conduct was approximately in February of 2023. Nevertheless, at all material times herein,

Defendants falsely represented to Plaintiff that their health information is not and will not be disclosed to any third party.

237. As alleged above, Defendants has a duty to disclose the nature and significance of its data disclosure practices but failed to do so. Defendants are therefore estopped from relying on any statute of limitations under the discovery rule.

CLASS ALLEGATIONS

238. **Class Definition:** Plaintiff brings this action on behalf of himself and on behalf of a class of persons similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.:

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

Nationwide Class: All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel on Defendants' Website.

240. The Vermont Subclass that Plaintiff seeks to represent is defined as:

Vermont Subclass: All individuals residing in the State of Vermont whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel on Defendants' Website.

241. The Nationwide Class and the Vermont Subclass are referred to throughout this Complaint as the "Class." Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendants has a controlling interest, any Defendants' officer or director, any successor or assign and any Judge who adjudicates this case, including their staff and immediate family.

242. **The following people are excluded from the Class:** (1) any Judge or Magistrate presiding over this action and members of their immediate families; (2) Defendant, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or its

parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

243. Plaintiff reserves the right under Federal Rule of Civil Procedure 23 to amend or modify the Class to include a broader scope, greater specificity, further division into subclasses, or limitations to particular issues. Plaintiff reserves the right under Federal Rule of Civil Procedure 23(c)(4) to seek certification of particular issues.

244. The requirements of Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3) are met in this case.

245. **Numerosity:** The exact number of Class Members is not available to Plaintiff, but it is clear that individual joinder is impracticable. Hundreds of thousands to millions of people have used Defendants' Website since at least 2016. Members of the Class can be identified through Defendants' records or by other means.

246. **Commonality:** Commonality requires that the Class Members' claims depend upon a common contention such that determination of its truth or falsity will resolve an issue that is central to the validity of each claim in one stroke. Here, there is a common contention for all Class Members as to whether Defendants disclosed to third parties their Private Information without authorization or lawful authority.

247. **Typicality:** Plaintiff's claims are typical of the claims of other Class Members in that Plaintiff and the Class Members sustained damages arising out of Defendants' uniform wrongful conduct and data sharing practices.

248. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff's claims are made in a representative capacity on behalf of the Class Members. Plaintiff has no interests antagonistic to the interests of the other Class Members. Plaintiff has retained competent counsel to prosecute the case on behalf of Plaintiff and the Class. Plaintiff and Plaintiff's counsel are committed to vigorously prosecuting this action on behalf of the Class members.

249. The declaratory and injunctive relief sought in this case includes:

- a. Entering a declaratory judgment against Defendants—declaring that Defendants' interception of Plaintiff's and Class Members' Private Information is in violation of the law;
- b. Entering an injunction against Defendants:
 - i. preventing Defendants from sharing Plaintiff's and Class Members' Private Information among themselves and other third parties;
 - ii. requiring Defendants to alert and/or otherwise notify all Users of their Website of what information is being collected, used, and shared;
 - iii. requiring Defendants to provide clear information regarding their practices concerning data collection from the Users/patients of Defendants' Website, as well as uses of such data;
 - iv. requiring Defendants to establish protocols intended to remove all personal information which has been leaked to Facebook and/or other third parties, and request Facebook/third parties to remove such information
 - v. and requiring Defendants to provide an opt out procedure for individuals who do not wish for their information to be tracked while interacting with Defendants' Website.

250. **Predominance:** There are many questions of law and fact common to the claims of Plaintiff and Class Members, and those questions predominate over any questions that may affect individual Class Members. Common questions and/or issues for Class members include, but are not necessarily limited to the following:

- a. Whether Defendants' unauthorized disclosure of Users' Private Information was negligent;
- b. Whether Defendants owed a duty to Plaintiff's and Class Members not to disclose their Private Information to unauthorized third parties;
- c. Whether Defendants breached its duty to Plaintiff and Class Members not to disclose their Private Information to unauthorized third parties;
- d. Whether Defendants represented to Plaintiff and the Class that they would protect Plaintiff's and the Class Members' Private Information;
- e. Whether Defendants violated Plaintiff's and Class Members' privacy rights;
- f. Whether Plaintiff and Class Members are entitled to actual damages, enhanced damages, statutory damages, and other monetary remedies provided by equity and law and
- g. Whether injunctive and declaratory relief, restitution, disgorgement, and other equitable relief is warranted.

251. **Superiority:** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by individual Class Members will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for the individual Class Members to obtain effective relief from Defendants' misconduct. Even if Class Members could mount such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort and expense will be enhanced, and uniformity of decisions ensured.

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

- a. Whether Defendants misrepresented that they would disclose personal information only for limited purposes that did not include purposes of delivering advertisements or collecting data for commercial use or supplementing consumer profiles created by data aggregators and advertisers;
- b. Whether Defendants' privacy policies misrepresented that they collected and shared User information with third-party service providers only for the limited purpose of providing access to its services;
- c. Whether Defendants misrepresented that they had in place contractual and technical protections that limit third-party use of User information and that it would seek User consent prior to sharing Private Information with third parties for purposes other than provision of its services;
- d. Whether Defendants misrepresented that any information they receive is stored under the same guidelines as any health entity that is subject to the strict patient data sharing and protection practices set forth in the regulations propounded under HIPAA;
- e. Whether Defendants misrepresented that they complied with HIPAA's requirements for protecting and handling Users' PHI;
- f. Whether Defendants breached their contractual obligations to not share Users' PHI without express written authorization;
- g. Whether Defendants shared the Private Information that Users provided to Defendants with advertising platforms, including Facebook, without adequate notification or disclosure, and without Users' consent, in violation of health privacy laws and rules and its own privacy policy;
- h. Whether Defendants integrated third-party tracking tools, such as Pixels, in its website that shared Private Information and User activities with third parties for unrestricted purposes, which included advertising, data analytics, and other commercial purposes;
- i. Whether Defendants shared Private Information and activity information with Facebook using Facebook's Pixels on its Website without Users' consent and

j. Whether Facebook used the information that Defendants shared with it for unrestricted purposes, such as selling targeted advertisements, data analytics, and other commercial purposes.

CLAIMS

COUNT ONE

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

18 U.S.C. § 2511(1), *et seq.*

Unauthorized Interception, Use and Disclosure

(On Behalf of Plaintiff & the Nationwide Class)

253. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

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

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

256. 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.

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

258. **Electronic Communications.** The transmission of PII and PHI between Plaintiff and Class Members and Defendants' 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).

259. **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).

260. Defendants’ intercepted communications include, but are not limited to, communications to/from Plaintiff and Class Members regarding PII and PHI, diagnosis of certain conditions, treatment/medication for such conditions, and scheduling of appointments, including treatment and diagnosis [REDACTED].

261. Furthermore, Defendants intercepted the “contents” of Plaintiff’s communications in at least the following forms:

- a. The parties to the communications;
- b. The precise text of patient search queries;
- c. PII such as patients’ IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;
- d. The precise text of patient communications about specific doctors;
- e. The precise text of patient communications about specific medical conditions;
- f. The precise text of information generated when patients requested or made appointments,
- g. The precise text of patient communications about specific treatments;
- h. The precise text of patient communications about scheduling appointments with medical providers;
- i. The precise text of patient communications about billing and payment;
- j. The precise text of specific buttons on Defendants’ Website that patients click to exchange communications including Log-Ins, Registrations, Requests for Appointments, Search, and other buttons;
- k. The precise dates and times when patients click to Log-In on Defendants’ Website;

l. The precise dates and times when patients visit Defendants' Website;

m. Information that is a general summary or informs third parties of the general subject of communications that Defendants sends back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment, and other information.

262. For example, Defendants' interception of the fact that a patient views a webpage like the following, involves "content," because it communicates that patient's request for the information on that page:

https://www.uvmhealth.org/medcenter/find-a-doctor?provider_name=emily+dalton&field_specialties_target_id=All&field_clinical_interests_target_id=All&field_provider_group_value=All&lat=&lng=&geolocation_geocoder_address=&field_geo_coordinates_proximity=2&field_locations_target_id=All&field_accepted_insurance_target_id=All&field_gender_value=All&field_languages_target_id=All

263. **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).

264. **Electronical, Mechanical or Other Device.** The ECPA defines "electronic, mechanical, or other device" as "any device ... which can be used to intercept a[n] ... electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

- a. The cookies Defendants and Meta use to track Plaintiff's and the Class Members' communications;
- b. Plaintiff's and Class Members' browsers;
- c. Plaintiff's and Class Members' computing devices
- d. Defendants' web servers and

e. The Pixel code deployed by Defendants to effectuate the sending and acquisition of patient communications.

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

266. Specifically, Defendants intercepted Plaintiff's and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Private Information to third parties such as Facebook.

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

268. This information was, in turn, used by third parties, such as Facebook to 1) place Plaintiff and Class Members in specific health-related categories and 2) target Plaintiff and Class Members with advertising associated with their specific health conditions.

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

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

271. Unauthorized Purpose. Defendants intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, violation of HIPAA and the causes of action described below, among others.

272. 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).

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

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

275. HIPAA defines IIHI as:

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

276. Plaintiff's and Class Members' information that Defendants disclosed to third parties qualifies as IIHI, and Defendants violated Plaintiff's expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6).

Defendants intentionally used the wire or electronic communications to intercept Plaintiff Private Information in violation of the law.

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

278. 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.

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

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

- a. Negligence;
- b. Breach of express contract;
- c. Breach of implied contract; and
- d. Breach of fiduciary duty.

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

know was receiving their information, and that Plaintiff and Class Members did not consent to receive this information.

282. Here, as alleged above, Defendants violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information to a third party.

283. As such, Defendants cannot viably claim any exception to ECPA liability.

284. Plaintiff and Class Members have suffered damages as a direct and proximate result of Defendants' invasion of privacy in that:

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

b. Defendants received substantial financial benefits from its use of Plaintiff's and the Class Members' PII and PHI without providing any value or benefit to Plaintiff or the Class members;

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

d. Defendants have failed to provide Plaintiff 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 its patient information and

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

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

286. Defendants were not acting under color of law to intercept Plaintiff's and the Class Members' wire or electronic communication.

287. Plaintiff and Class Members did not authorize Defendants to acquire the content of their communications for purposes of invading their privacy via the Pixel.

288. Any purported consent that Defendants received from Plaintiff and Class Members was not valid.

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

290. Defendants' scheme or artifice to defraud in this action consists of:

- a. the false and misleading statements and omissions in its privacy policy set forth above, including the statements and omissions recited above; and
- b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie on Defendants' Website rather than a third-party cookie from Facebook.

291. Defendants acted with the intent to defraud in that it willfully invaded and took Plaintiff's and Class Members' property:

- a. property rights to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and
- b. property rights to determine who has access to their computing devices.

292. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendants' Website, Defendants' purpose was

tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

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

COUNT TWO

BREACH OF EXPRESS CONTRACT *(On behalf of Plaintiff & the Nationwide Class)*

294. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

295. Plaintiff and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with Defendants for the provision of medical and health care services.

296. Specifically, Plaintiff and Class Members entered into a valid and enforceable express contract with Defendants when Plaintiff first received medical care from Defendant.

297. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with Defendants include Defendants' promise to protect nonpublic, Private Information given to Defendants or that Defendants gathers on their own from disclosure.

298. Under these express contracts, Defendants and/or their affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff and the Class Members' PII/PHI: (i) provided to obtain such healthcare;

and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

299. Both the provision of medical services and the protection of Plaintiff and Class Members' Private Information were material aspects of these express contracts.

300. The express contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Defendants' Privacy Notice.

301. At all relevant times, Defendants expressly represented in its Privacy Notice, among other things: (i) that “We understand the importance of safeguarding personal information and are committed to protecting your privacy.”; and (ii) that “You may use this Web site without providing any personal information (e.g., your name, address, or phone number). We only obtain personal information if you choose to provide it to us.”⁷³

302. Defendants' express representations, including, but not limited to, express representations found in their Privacy Notice, formed and embodied an express contractual obligation requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

303. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

⁷³ <https://web.archive.org/web/20201124092625/https://www.uvmhealth.org/privacy-policy> last visited Apr. 16, 2024).

304. Plaintiff and Class Members would not have entered into these contracts with Defendants and/or their affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

305. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendants and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

306. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

307. Defendants materially breached its contractual obligation to protect the nonpublic Private Information Defendants gathered when it disclosed that Private Information to Meta through the Meta Collection Tools, including the Meta Pixel on its Website.

308. Defendants materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendants did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by Defendants' sharing of that Private Information with Meta through the Meta Collection Tools, including the Meta Pixel on its Website.

309. The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Meta, was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

310. As a result of Defendants' failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain,

and instead received healthcare and other services that were of a diminished value to that described in the contracts.

311. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

312. Had Defendants disclosed that their data privacy was inadequate or that they did not adhere to industry-standard privacy measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendants and/or their affiliated healthcare providers.

313. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Meta, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

314. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Meta.

COUNT THREE

BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING *(On behalf of Plaintiff & the Nationwide Class)*

315. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

316. Plaintiff and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with Defendants for the provision of medical and health care services.

317. Specifically, Plaintiff and Class Members entered into a valid and enforceable express contract with Defendants when Plaintiff first received medical care from Defendant.

318. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with Defendants include Defendants' implied duty of good faith and fair dealing, particularly due to Defendants' special relationship with Plaintiff as their healthcare provider.

319. Under these express contracts, Defendants and/or their affiliated healthcare providers, promised and were obligated to provide healthcare to Plaintiff and Class Members. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

320. In service of its implied duty of good faith and fair dealing when executing the contract, Defendants was bound to not voluntarily divulge Plaintiff's and Class Members' sensitive, non-public Private Information to third parties for monetary gain without Plaintiff's and Class Members' consent to such disclosures.

321. The express contracts for the provision of medical services are formed and embodied in multiple documents.

322. As evidence of Defendants' knowledge of its obligations to perform the contracts in accordance with its implied duty of good faith and fair dealing and Plaintiff's expectations of Defendants to do the same, at all relevant times, Defendants expressly represented in its Privacy Notice, among other things: (i) that "We understand the importance of safeguarding personal

information and are committed to protecting your privacy.”; and (ii) that “You may use this Web site without providing any personal information (e.g., your name, address, or phone number). We only obtain personal information if you choose to provide it to us.”⁷⁴

323. Defendants’ express representations, including, but not limited to, express representations found in their Privacy Notice, evidence Defendants’ knowledge of the specific manifestations of its duty to perform the contracts in accordance with its implied duty of good faith and fair dealing, which required Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff’s and Class Members’ Private Information.

324. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

325. Plaintiff and Class Members would not have entered into these contracts with Defendants and/or their affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

326. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendants and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and, through Defendants’ implied duty of good faith and fair dealing, the protection of their Private Information.

⁷⁴ *Id.*

327. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

328. Defendants did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by Defendants' sharing of that Private Information with Meta through the Meta Collection Tools, including the Meta Pixel on its Website.

329. Defendants breached its implied duty of good faith and fair dealing to protect the nonpublic Private Information Defendants gathered when it disclosed that Private Information to Meta through the Meta Collection Tools, including the Meta Pixel on its Website.

330. The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Meta, was a reasonably foreseeable consequence of Defendants' actions in breach of its implied duty of good faith and fair dealing.

331. As a result of Defendants' failure to fulfill the data privacy protections inherent in the special relationship with Plaintiff and the Class Members and resulting breach of its implied duty of good faith and fair dealing, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts.

332. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

333. Had Defendants disclosed that their data privacy was inadequate or that they did not adhere to industry-standard privacy measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendants and/or their affiliated healthcare providers.

334. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Meta, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

335. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Meta.

COUNT FOUR

BREACH OF IMPLIED CONTRACT *(On behalf of Plaintiff & the Nationwide Class)*

336. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

337. Plaintiff and Class Members allege they entered into valid and enforceable implied contracts or were third-party beneficiaries of valid and enforceable implied contracts, with Defendants for the provision of medical and health care services.

338. Specifically, Plaintiff and Class Members entered into a valid and enforceable contract with Defendants when Plaintiff first received medical care from Defendant.

339. The valid and enforceable contracts to provide medical and health care services that Plaintiff and Class Members entered into with Defendants include Defendants' promise to protect nonpublic, Private Information given to Defendants or that Defendants gathers on their own from disclosure.

340. Under these contracts, Defendants and/or their affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

341. Both the provision of medical services and the protection of Plaintiff and Class Members' Private Information were material aspects of these contracts.

342. The contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Defendants' Privacy Notice.

343. At all relevant times, Defendants expressly represented in its Privacy Notice, among other things: (i) that “We understand the importance of safeguarding personal information and are committed to protecting your privacy.”; and (ii) that “You may use this Web site without providing any personal information (e.g., your name, address, or phone number). We only obtain personal information if you choose to provide it to us.”⁷⁵

344. Defendants' express representations, including, but not limited to, express representations found in their Privacy Notice, formed and embodied an express contractual obligation requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

345. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To

⁷⁵ *Id.*

customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entered into these contracts with Defendants and/or their affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

346. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendants and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

347. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

348. Defendants materially breached its contractual obligation to protect the nonpublic Private Information Defendants gathered when it disclosed that Private Information to Meta through the Meta Collection Tools, including the Meta Pixel on its Website.

349. Defendants materially breached the terms of these contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendants did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by Defendants' sharing of that Private Information with Meta through the Meta Collection Tools, including the Meta Pixel on its Website.

350. The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Meta, was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

351. As a result of Defendants' failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

352. Had Defendants disclosed that their data privacy was inadequate or that they did not adhere to industry-standard privacy measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendants and/or their affiliated healthcare providers.

353. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Meta, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

354. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Meta.

COUNT FIVE
NEGLIGENCE
(On behalf of Plaintiff & the Nationwide Class)

355. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

356. Defendants required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare services.

357. Upon accepting, storing, and controlling the Private Information of Plaintiff and the Class in its computer systems, Defendants owed, and continues to owe, a duty to Plaintiff and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information from disclosure to third parties.

358. Defendants' duty of care to use reasonable measures to secure and safeguard Plaintiff's and Class Members' Private Information arose due, in part, to the special relationship that existed between Defendants and its patients, which is recognized by statute, regulations, and the common law.

359. In addition, Defendants had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

360. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or

disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1).

361. Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes “protected health information” within the meaning of HIPAA.

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

363. Defendants’ duty to use reasonable care in protecting confidential data arose also because Defendants is bound by industry standards to protect confidential Private Information.

364. Defendants breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff’s and Class Members’ Private Information from unauthorized disclosure.

365. It was reasonably foreseeable that Defendants’ failures to exercise reasonable care in safeguarding and protecting Plaintiff’s and Class members’ Private Information through its use of the Meta Pixels and other tracking technologies would result in unauthorized third parties, such as Facebook, gaining access to such Private Information for no lawful purpose.

366. Defendants’ own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information.

367. Defendants’ misconduct included the failure to (1) secure Plaintiff’s and Class Members’ Private Information; (2) comply with industry standard data security practices; (3) implement adequate website and event monitoring; (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Meta Pixels and other tracking technologies; and (5) prevent unauthorized access to Plaintiff’s and Class

Members' Private Information by sharing that information with Meta and other third parties. Defendants' failures and breaches of these duties constituted negligence.

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

369. Defendants' wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiff's and Class members' Private Information constituted (and continue to constitute) negligence at common law.

370. Plaintiff and Class Members are entitled to compensatory, nominal, and/or punitive damages, and Plaintiff and Class Members are entitled to recover those damages in an amount to be determined at trial.

371. Defendants' negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner. Therefore, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen its data security systems and monitoring procedures; (ii) cease sharing Plaintiff's and Class Members' Private Information with Meta and other third parties without Plaintiff's and Class Members' express consent; and (iii) submit to future annual audits of its security systems and monitoring procedures.

COUNT SIX
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff & the Nationwide Class)

372. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

373. In light of the special physician-patient relationship between Defendants and Plaintiff and Class Members, which was created for the purpose of Defendants providing healthcare to Plaintiff and Class Members, Defendants became guardian of Plaintiff's and Class Members' Private Information. Defendants became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and does store.

374. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its patients and former patients, in particular, to keep secure their Private Information.

375. Defendants breached its fiduciary duties to Plaintiff and Class Members by disclosing their Private Information to unauthorized third parties, including Meta, and separately, by failing to notify Plaintiff and Class Members of this fact.

376. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injury and are entitled to compensatory, nominal, and/or punitive damages, and disgorgement of profits, in an amount to be proven at trial.

COUNT SEVEN
UNJUST ENRICHMENT
(On behalf of Plaintiff & Nationwide Class)

377. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein, except for the paragraphs specifically regarding breach of contract.

378. Plaintiff pleads this claim in the alternative to their breach of contract claim.

379. Plaintiff and Class Members personally and directly conferred a benefit on Defendants by paying Defendants for health care services, which included Defendants' obligation to protect Plaintiff's and Class Members' Private Information. Defendants were aware of Plaintiff's privacy expectations, and in fact, promised to maintain Plaintiff's Private Information confidential and not to disclose to third parties. Defendants received payments for medical services from Plaintiff and Class Members.

380. Plaintiff and Class Members also conferred a benefit on Defendants in the form of valuable sensitive medical information that Defendants collected from Plaintiff and Class Members under the guise of keeping this information private.

381. Defendants collected, used, and disclosed this information for its own gain, including for advertisement, market research, sale, or trade for valuable benefits from Facebook and other third parties.

382. Defendants had knowledge that Plaintiff and Class Members had conferred this benefit on Defendants by interacting with its Website, and Defendants intentionally installed the Meta Pixel tool on its Website to capture and monetize this benefit conferred by Plaintiff and Class Members.

383. Plaintiff and Class Members would not have used Defendants' Website had they known that Defendants would collect, use, and disclose this information to Facebook, Google, and other third parties.

384. The services that Plaintiff and Class Members ultimately received in exchange for the monies paid to Defendants were worth quantifiably less than the services that Defendants promised to provide, which included Defendants' promise that any patient communications with Defendants would be treated as confidential and would never be disclosed to third parties for marketing purposes without the express consent of patients.

385. The medical services that Defendants offers are available from many other health care systems that do protect the confidentiality of patient communications. Had Defendants disclosed that it would allow third parties to secretly collect Plaintiff's and Class Members' Private Health Information without consent, neither Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendants and/or its affiliated healthcare providers.

386. By virtue of the unlawful, unfair and deceptive conduct alleged herein, Defendants knowingly realized hundreds of millions of dollars in revenue from the use of the Private Information of Plaintiff and Classes Members for profit by way of targeted advertising related to Users' respective medical conditions and treatments sought.

387. This Private Information, the value of the Private Information, and/or the attendant revenue, were monetary benefits conferred upon Defendants by Plaintiff and Class Members.

388. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages in the loss of value of their Private Information and the lost profits from the use of their Private Information.

389. It would be inequitable and unjust to permit Defendants to retain the enormous economic benefits (financial and otherwise) it has obtained from and/or at the expense of Plaintiff and Class Members.

390. Defendants will be unjustly enriched if it is permitted to retain the economic benefits conferred upon them by Plaintiff and Class Members through Defendants' obtaining the Private Information and the value thereof, and profiting from the unlawful, unauthorized and impermissible use of the Private Information of Plaintiff and Class Members.

391. Plaintiff and Class Members are therefore entitled to recover the amounts realized by Defendants at the expense of Plaintiff and Class Members.

392. Plaintiff and the Class Members have no adequate remedy at law and are therefore entitled to restitution, disgorgement, and/or the imposition of a constructive trust to recover the amount of Defendants' ill-gotten gains, and/or other sums as may be just and equitable.

COUNT EIGHT
VERMONT CONSUMER PROTECTION ACT
9 V.S.A. § 2451 *et seq.*
(On behalf of Plaintiff & the Vermont Subclass)

393. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein, except for the paragraphs specifically regarding breach of contract.

394. Defendants are "sellers" as defined by 9 V.S.A. § 2451a(3), engaged in the business of offering services to consumers.

395. Plaintiff and the Vermont Subclass Members are "consumers" as defined by 9 V.S.A. § 2451a(1) who paid consideration for services to Defendants.

396. Defendants' unfair acts and practices against Plaintiff and the Vermont Subclass Members occurred in the course of trade or commerce in Vermont, arose out of transactions that occurred in Vermont, and/or harmed individuals in Vermont.

397. Plaintiff and the Vermont Subclass Members received and paid for health care services from Defendants.

398. Plaintiff and the Vermont Subclass Members used Defendants' Website in connection with receiving health care services from Defendants.

399. Plaintiff's and the Vermont Subclass Members' payments to Defendants for health care services were for household and personal purposes.

400. Defendants' practices of disclosing Plaintiff's and the Vermont Subclass Members' PII and PHI by re-directing confidential communications via the Meta Pixel to third parties without authorization, consent, or knowledge of Plaintiff and the Vermont Subclass Members is a deceptive, unfair, and unlawful trade act or practice, in violation of 9 V.S.A. § 2451(a).

401. Defendants' unfair business practices were targeted at all of Defendants' customers, including Plaintiff and the Vermont Subclass Members.

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

403. Defendants intended to mislead Plaintiff and the Vermont Subclass Members and to induce them to rely on its misrepresentations and omissions.

404. Defendants' surreptitious collection and disclosure of Plaintiff's and the Vermont Subclass Members' PII, PHI, and communications to third parties involves important consumer protection concerns.

405. Defendants represented that they would safeguard and protect Plaintiff's and Vermont Subclass Members' Private Information, in their Privacy Policy and elsewhere, to keep such information secure and confidential.⁷⁶

406. Defendants made these representations with the intent to induce Plaintiff and Vermont Subclass Members to seek health care services from Defendants and to use Defendants' Website in doing so.

407. Plaintiff and Vermont Subclass Members relied upon Defendants' representations in seeking health care services from Defendants and in using Defendants' Website to obtain such services.

408. As a direct and proximate cause of Defendants' unfair acts and practices, Plaintiff and Vermont Subclass Members have suffered actual damages.

409. Plaintiff's and the Vermont Subclass Members' injuries were proximately caused by Defendants' unfair and deceptive business practices.

410. As a result of Defendants' conduct, Defendants has been unjustly enriched.

411. Defendants' acts caused substantial injury that Plaintiff and the Vermont Subclass Members could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

412. Defendants acted intentionally, knowingly, and maliciously to violate Vermont's Consumer Protection Act, and recklessly disregarded Plaintiff's and the Vermont Subclass Members' rights.

⁷⁶ See *The University of Vermont Health Network Web Site Privacy Policy*, <https://web.archive.org/web/20170428064038/https://www.uvmhealth.org/pages/privacy-policy.aspx> (last visited Apr. 16, 2024).

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

414. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive acts and practices, Plaintiff and the Vermont Subclass Members were also damaged by Defendants' conduct in that:

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

415. As a direct and proximate result of Defendants' above-described violation of the Vermont Consumer Protection Act, Plaintiff and Vermont Subclass Members are entitled to recover actual damages, reasonable attorneys' fees, and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the Proposed Classes defined herein, respectfully requests this Honorable Court to provide the following relief:

A. That this Action be maintained as a Class Action, that Plaintiff be named as Class Representative of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order:

1. Preventing Defendants from sharing Plaintiff's and Class Members' Private Information among other third parties;

2. Requiring Defendants to alert and/or otherwise notify all Users of its Website of what information is being collected, used, and shared;

3. Requiring Defendants to provide clear information regarding its practices concerning data collection from the Users/patients of Defendants' Website, as well as uses of such data;

4. Requiring Defendants to establish protocols intended to remove all personal information which has been leaked to Facebook and/or other third parties, and request Facebook/third parties to remove such information;

5. Requiring Defendants to provide an opt out procedure for individuals who do not wish for their information to be tracked while interacting with Defendants' Website;

6. Mandating the proper notice be sent to all affected individuals, and posted publicly;

7. Requiring Defendants to delete, destroy, and purge the Private Information of Users unless Defendants can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Users;

8. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

C. That the Court award Plaintiff and the Class Members damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

D. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendants to which Plaintiff and the Class are entitled, including but not limited to restitution and an Order requiring Defendants to cooperate and financially support civil and/or criminal asset recovery efforts;

E. Plaintiff and the Class be awarded with pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

F. Plaintiff and the Class be awarded with the reasonable attorneys' fees and costs of suit incurred by their attorneys;

G. Plaintiff and the Class be awarded with treble and/or punitive damages insofar as they are allowed by applicable laws; and

H. Any and all other such relief as the Court may deem just and proper under the circumstances.

JURY TRIAL DEMANDED

Plaintiff demands a jury trial on all triable issues.

DATED: June 20, 2024

Respectfully submitted,



Wendy E. Radcliff (ERN 10126)
LANGROCK SPERRY & WOOL
111 South Pleasant Street
Middlebury, VT 05753
P: 802.989.7834
wradcliff@langrock.com

Matthew J. Langley
(*pro hac vice* admission to be sought)
David S. Almeida
(*pro hac vice* admission to be sought)
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024 (phone)
david@almeidalawgroup.com

Nicholas A. Migliaccio
(*pro hac vice* to be sought)
Jason S. Rathod
(*pro hac vice* to be sought)
MIGLIACCIO & RATHOD LLP
412 H St NE, Suite 302
Washington DC 20002
Telephone (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Attorneys for Plaintiff