UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

ROBERT CHRISTENSEN and MARTHA RUSSELL, individually and on behalf of all others similarly situated, Plaintiffs, v. MEDICAL SCANNING CONSULTANTS, P.A. d/b/a Center for Diagnostic Imaging d/b/a Rayus Radiology and DIAGNOSTIC SERVICES HOLDINGS, INC. d/b/a Rayus Radiology, Defendants.	Case No. **CLASS ACTION COMPLAINT** Jury Trial Demanded

Plaintiffs Robert Christensen and Martha Russell, individually and on behalf of all others similarly situated (hereinafter "Plaintiffs"), bring this Class Action Complaint against Defendant Medical Scanning Consultants, P.A. d/b/a Center for Diagnostics Imaging d/b/a Rayus Radiology and Defendant Diagnostic Services Holdings, Inc. d/b/a Rayus Radiology (collectively "Defendants" or "Rayus Radiology"), and allege, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this case to address Defendants' illegal, and widespread practice of disclosing Plaintiffs' and Class Members' confidential personally identifiable

information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information") to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook") and other third parties (the "Disclosure").

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

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

4. Rayus Radiology "is one of the nation's leading providers of high-quality diagnostic imaging and interventional radiology services," with a network of 22 locations in Minnesota alone.[1]

5. In spite of their unique position as a massive and trusted healthcare provider, Rayus Radiology knowingly configured and implemented a software device known as a Tracking Pixel ("Pixel") to collect and transmit information from https://rayusradiology.com/ (the "Website") to third parties, including information communicated in sensitive and presumptively confidential patient searches for providers, locations, and healthcare services through Defendants' Website and associated web properties and information communicated through Defendants' online billing portal (collectively the "Online Platforms").

6. Defendants encourage patients to use their Online Platforms for locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, making medical appointments, checking test results, paying for medical services, and more.

7. Plaintiffs and other Class Members who used Defendants' Website thought they were communicating only with their trusted healthcare provider. Unbeknownst to Plaintiffs and Class Members, however, Defendants have embedded a Tracking Pixel, such as the Facebook Tracking Pixel (the "Facebook Pixel"), on their Online Platforms,

[1] *Twin Cities, Minnesota*, RAYUS RADIOLOGY, https://rayusradiology.com/market-twin-cities-minnesota/ (last visited June 28, 2023); *Central Minnesota*, RAYUS RADIOLOGY, https://rayusradiology.com/market-central-minnesota/ (last visited June 28, 2023).

surreptitiously forcing Plaintiffs and Class Members to transmit to Facebook and other third parties every click, keystroke, and intimate detail about their medical treatment. Operating as designed and as implemented by Defendants, the Pixel allows the Private Information that Plaintiffs and Class Members submit to Defendants to be unlawfully disclosed to Facebook and other third parties alongside the individual's IP address and unique and persistent Facebook ID ("FID").[2]

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

9. The user's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Tracking Pixel is thus customizable and programmable, meaning that the website owner controls which of its pages contain the Pixel and which events are tracked and transmitted to Facebook and other third-party tracking technology vendors. By

[2] The Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." *What are cookies?*, CLOUDFLARE, https://www.cloudflare.com/learning/privacy /what-are-cookies/ (last visited Mar. 21, 2023). "Cookies help inform websites about the user, enabling the websites to personalize the user experience." *Id.*

[3] *Retargeting*, FACEBOOK, https://www.facebook.com/business/goals/retargeting (last visited Mar. 21, 2023).

installing the Tracking Pixel on their Website, Defendants effectively planted a bug on Plaintiffs' and Class Members' web browsers and compelled them to disclose their communications with Defendants to Facebook and other likely third parties.

10. In addition to the Facebook Pixel, Defendants also likely installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on their Website servers.[4]

11. Unlike the Facebook Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[5] Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to

[4] "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir ElKamouny, *How to Implement Facebook Conversions API (In Shopify)*, FETCH&FUNNEL, https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Mar. 21, 2023).

[5] *What is the Facebook Conversion SPI and How to Use It*, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last visited Mar. 21, 2023). "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel . . . . This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." *Conversions API*, META FOR DEVELOPERS, https://developers.facebook. com/docs/marketing-api/conversions-api (last visited Mar. 21, 2023).

conversion. This helps you better understand how digital advertising impacts both online and offline results."[6]

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

13. Defendants utilized the Tracking Pixel and CAPI data for marketing purposes in an effort to bolster its profits. The Tracking Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiffs' and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendants.

14. The information that Defendants' Tracking Pixel and CAPI sent to Facebook and other third parties included the Private Information that Plaintiffs and Class Members submitted to Defendants' Online Platforms, including for example, the type of medical treatment sought, the individual's particular health condition, the fact that the individual attempted to or did book a medical appointment, and that the individual attempted to or did pay Defendants for medical services.

15. Such information allows a third-party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiffs' and Class

[6] *About Conversions API*, META, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Mar. 21, 2023).

Members' Private Information to third-party marketers who online target[7] Plaintiffs' and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and CAPI. Facebook and any third-party purchasers of Plaintiffs' and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition.

16. Healthcare patients simply do not anticipate that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patient's consent. Neither Plaintiffs nor any other Class Member signed a written authorization permitting Defendants to send their Private Information to Facebook or other third-party tracking technology vendors.

17. Despite willfully and intentionally incorporating the Tracking Pixel and likely CAPI into their Website and servers, Defendants have never disclosed to Plaintiffs or Class Members that they shared their sensitive and confidential communications and Private Information with Facebook and other likely third parties. Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook as they communicated with their healthcare provider via the Online Platforms,

[7] "Online Targeting" is "a process that refers to creating advertisement elements that specifically reach out to prospects and customers interested in offerings. A target audience has certain traits, demographics, and other characteristics, based on products or services the advertiser is promoting." *See A Guide to Online Targeting – Which Works For Your Business*, DIGITAL MARKETING GROUP, https://digitalmarketinggroup.com/a-guide-to-online-targeting-which-works-for-your-business/ (last visited June 23, 2023).

or stored on Defendants' servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes.

18. Defendants further made express and implied promises to protect Plaintiffs' and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendants.

19. Defendants owed common law, statutory, and regulatory duties to keep Plaintiffs' and Class Members' communications and medical information safe, secure, and confidential.

20. Upon information and belief, Defendants utilized the Pixel data to improve and to save costs on its marketing campaigns, improve its data analytics, and attract new patients.

21. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties to those individuals to protect and to safeguard that information from unauthorized disclosure.

22. However, as set forth more fully below, Defendants failed in their obligations and promises by using Tracking Pixels while knowing that doing so would result in the transmission and disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties with a long history of privacy violations and misconduct—*i.e.* Facebook.

23. Plaintiffs and Class Members Private Information can—and likely will—be further exploited and disseminated for retargeting, marketing, or insurance companies utilizing the information to set insurance rates.

24. Defendants breached its statutory and common law obligations to Plaintiffs and Class Members by, *inter alia*: (i) failing to adequately review their marketing programs and web based technology to ensure the Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) aiding, agreeing, and conspiring with third-parties to intercept communications sent and received by Plaintiffs and Class Members; (iv) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook or others; (v) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through Tracking Pixels; (vi) failing to warn Plaintiffs and Class Members; and (vii) otherwise failing to design and monitor their Website to maintain the confidentiality and integrity of patient Private Information.

25. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) invasion of privacy, (ii) loss of benefit of the bargain, (iii) diminution or deprivation of value of the Private Information, (iv) statutory damages, and (v) the continued and ongoing risk of exposure of their Private Information.

26. Plaintiffs seek to remedy these harms and brings causes of action for: (I) Negligence, (II) Negligence Per Se, (III) Invasion of Privacy – Publication of Private Facts, (IV) Invasion of Privacy – Intrusion Upon Seclusion; (V) Breach of Implied Contract, (VI) Unjust Enrichment, (VII) Breach of Fiduciary Duty; (VIII) Violation of the Texas Medical

Practices Act; (IX) Violation of the Tennessee Consumer Protection Act of 1977; (X) Violation of the Tennessee Wiretapping and Electronic Surveillance Act; (XI) Violation of the Minnesota Uniform Deceptive Trade Practices Act; (XII) Violation of the Minnesota Consumer Fraud Act; and (XIII) Violation of the Minnesota Health Records Act.

THE PARTIES

27. Plaintiff Robert Christensen is a natural person, resident, and citizen of Texas. He has no intention of moving to a different state in the immediate future. Plaintiff is a former patient of Rayus Radiology.

28. Plaintiff Martha Russell is a natural person, resident, and citizen of Tennessee. She has no intention of moving to a different state in the immediate future. Plaintiff is a current patient of Rayus Radiology.

29. Defendant Medical Scanning Consultants, P.A. d/b/a Center for Diagnostic Imaging d/b/a Rayus Radiology is a professional association organized and existing under the laws of the State of Minnesota, with a principal place of business at 5775 Wayzata Boulevard, Suite 400, St. Louis Park, Minnesota, 55416.

30. Defendant Diagnostic Services Holdings, Inc. d/b/a Rayus Radiology is a corporation organized and existing in the State of Delaware with a principal place of business at 5775 Wayzata Boulevard, Suite 400, St. Louis Park, Minnesota, 55416.

JURISDICTION AND VENUE

31. This Court 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 100 putative class members defined

below, and minimal diversity exists because a significant portion of the putative class members are citizens of a state different from the citizenship of at least one Defendant.

32. This Court has jurisdiction over Defendants because they engage in a continuous and systematic course of business and maintain their principal places of business within Hennepin County, Minnesota.

33. In accordance with 28 U.S.C. § 1391, venue is proper in this District because Defendants conducts substantial business and maintain their principal place of business in this District and a substantial part of the events and conduct giving rise to Plaintiffs' and the Class Members' claims emanated from activities within this District.

COMMON FACTUAL ALLEGATIONS

A. Background

34. Defendant Diagnostic Services Holdings, Inc. is the parent company of the "RAYUS Radiology network" and "works along with its local and regional affiliates to manage the RAYUS Radiology website network."[8]

35. Defendants offer radiological services, including bone density testing, computerized tomography ("CT") scans, breast imaging, pain care, nuclear medicine, interventional and vascular radiology, magnetic resonance imaging ("MRI") testing, injections and biopsies, PET/CT examinations, ultrasounds, x-rays, and electrocardiograms

[8] *Terms of Use*, RAYUS RADIOLOGY, https://rayusradiology.com/terms-of-use/ (last visited June 29, 2023).

("EKGs"), to patients through hospitals, clinics, and other health care facilities across the country.[9]

36. Defendants claim to be "a leader in advanced diagnostic and interventional radiology," with over 400 radiologists, 1.2 million annual images performed, and 150 current clinical trials. [10]

37. Defendants serve many of their patients via their Online Platforms, which they encourage patients to use for locating physicians and treatment facilities, researching and selecting medical conditions and services, searching for medical information published by Defendants through blogs and articles, paying for medical services, communicating with providers, scheduling appointments and procedures, and communicating other information related to their treatment and status as a patient.

38. Defendants use their Website to connect Plaintiffs and Class Members to Defendants' digital healthcare platform with the goal of increasing profitability.

39. In furtherance of that goal, and to increase the success of its advertising and marketing, Defendants purposely installed the Tracking Pixels on their Website to advertise their services to Plaintiffs and Class Members. In doing so, Defendants surreptitiously tracked, recorded, transmitted, and disseminated its patients' private and protected communications with Facebook and other third parties, including communications that contain Plaintiffs' and Class Members' Private Information.

---

[9] *Services*, RAYUS RADIOLOGY, https://rayusradiology.com/services/ (last visited June 29, 2023).

[10] *Rayus Radiology*, RAYUS RADIOLOGY, https://rayusradiology.com/ (last visited June 29, 2023).

40. While seeking and using Defendants' services as a medical provider via their Website, Plaintiffs' and Class Members' Private Information was intercepted by third parties via the Tracking Pixels, and it was also transmitted to third parties by Defendants via first-party cookies and conversions API tools.

41. Plaintiffs and Class Members did not intend or have any reason to suspect the Private Information would be shared with Facebook or other third parties, or that Defendants were tracking their every communication and disclosing the same to third parties when they entered highly sensitive information on Defendants' Website.

42. Plaintiffs and Class Members never consented, agreed, authorized, or otherwise permitted Defendants to disclose their Private Information.

43. Upon information and belief, Defendants intercepted and disclosed Plaintiffs' and Class Members': (1) status as medical patients; (2) communications with Defendants through its Website; and (3) information about their medical appointments, location of treatments, specific medical providers, specific medical conditions and treatments, and related information.

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

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

i. Facebook's Business Tools and the Pixel

46. Facebook operates the world's largest social media company, which generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[11]

47. As a core part of its business, Facebook maintains profiles on users that include the user's real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers, including IP addresses.

48. Facebook also tracks non-Facebook users through its widespread internet marketing products and source code.

49. Facebook then sells advertising space by highlighting its ability to target users.[12] Facebook can target users so effectively because it surveils user activity both on and off its site.[13] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[14] Facebook compiles this information into a generalized dataset called "Core Audiences," which

---

[11] *Meta Reports Fourth Quarter and Full Year 2021 Results*, META INVESTOR RELATIONS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Dec. 2, 2022).

[12] *Why Advertise on Facebook, Instagram, and other Meta technologies*, META, https://www.facebook.com/business/help/205029060038706 (last visited June 23, 2023).

[13] *About Meta Pixel*, META, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited June 23, 2023).

[14] *Audience ad targeting*, META, https://www.facebook.com/business/ads/ad-targeting (last visited June 23, 2023).

advertisers use to apply highly specific filters and parameters for their targeted advertisements.[15]

50. Indeed, Facebook utilizes the precise type of information disclosed by Defendants to identify, target, and market products and services to individuals.

51. Advertisers can also build "Custom Audiences."[16] Custom Audiences enable advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[17] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[18] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools," including the Facebook Pixel.[19]

---

[15] *Core-Audiences*, META, https://www.facebook.com/business/news/Core-Audiences (last visited June 23, 2023).

[16] *About custom audiences*, META, https://www.facebook.com/business/help/74435470 8981227?id=2469097953376494 (last visited June 23, 2023).

[17] *Audience ad targeting*, *supra* note 16.

[18] *About lookalike audiences*, META, https://www.facebook.com/business/help/ 164749007013531?id=401668390442328 (last visited June 23, 2023).

[19] *Create a customer list Custom Audience*, META, https://www.facebook.com/ business/help/170456843145568?id=2469097953376494 (last visited June 23, 2023); *Create a website custom audience*, META, https://www.facebook.com/business/help/1474662202748 341?id=2469097953376494 (last visited June 23, 2023).

52. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[20] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept, collect, view, and use user activity on those platforms.

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

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

55. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[21] Businesses

[20] *The Meta Business Tools*, META, https://www.facebook.com/help/331509497253087 (last visited June 23, 2023).

[21] *Specifications for Meta Pixel Standard Events*, FACEBOOK, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Mar. 21, 2023); *see Facebook Pixel, Accurate Event Tracking, Advanced*, FACEBOOK, https://developers.facebook. com/docs/meta-pixel/advanced (last visited Mar. 21, 2023); *see also Best Practices for Meta Pixel Setup*, FACEBOOK, https://www.facebook.com/business/help/218844828315224?id=1205376682 832142

that want to target customers and advertise their services, such as Defendants, can track other user actions and can create their own tracking parameters by building a "custom event."[22]

56. One such Business Tool is the Facebook Pixel. Facebook offers this piece of code to advertisers, like Defendants, to integrate into their websites. As the name implies, the Facebook Pixel "tracks the people and the types of actions they take."[23] When a user accesses a website hosting the Facebook Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers at certain times during interaction with the webpage. This second, secret transmission contains the original request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendants' Websites—Defendants' own code, and Facebook's embedded code.

57. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients' Facebook IDs, IP addresses, and/or device IDs and the other information they input into Defendants' Website, including not only their medical searches, treatment requests, and the webpages they view, but also their home address, zip code, or

---

(last visited Mar. 21, 2023); *App Events API*, FACEBOOK, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Mar. 21, 2023).

[22] *About Standard and Custom Website Events*, FACEBOOK, https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (last visited Mar. 21, 2023); *see also App Events API*, *supra* note 23.

[23] *Retargeting*, *supra* note 3.

phone number. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[24] Plaintiffs' and Class Members identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

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

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

60. Notably, this transmission only occurs on webpages that contain a Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't

[24] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited June 23, 2023).

implicate privacy and disable it on pages that do implicate patient privacy. Thus, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook or other third parties via the Tracking Pixels but for Defendants' decisions to install the Pixel on its Website and specifically on webpages that solicit and receive Private Information.

61. Similarly, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook via Conversions API but for Defendants' decision to install and implement that tool on their servers.

62. By installing and implementing both tools, Defendants caused Plaintiffs' and Class Members' communications to be intercepted and transmitted from Plaintiffs' and Class Members' browsers directly to Facebook via the Pixel, or to be recorded on Defendants' servers and then transferred to Facebook via Conversions API.[25]

ii. Defendants' method of transmitting Plaintiffs' and Class Members' Private Information via the Tracking Pixel and/or Conversion API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Pixel

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

[25] Facebook assigns a unique "event_id" parameter to each separate communication with a website and then duplicates the data based on the event_id so that the same event tracked by the Pixel and recorded by the CAPI are not reported as two separate events. *Set Up Conversions API for Server-Side Tagging in Google Tag Manager*, FACEBOOK, https://www.facebook.com/ business/help/702509907046774 (last visited Mar. 21, 2023).

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

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

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

66. When an individual visits Defendants' Website, their web browser sends an HTTP Request to Defendants' servers that essentially asks Defendants' Website to retrieve

certain information (such as Defendants' "Services" and "Locations" pages). Defendants' servers send the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendants' Website.

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

68. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendants' Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When patients visit Defendants' website via an HTTP Request to Defendants' server, Defendants' server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendants' Pixel. Thus, Defendants are in essence handing patients a tapped phone, and once the Webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendants and transmits those communications to third-parties, including Facebook.

69. Separate from the Pixel, Facebook and other website owners can place third-party cookies in the web browsers of users logged into their websites or services. These cookies can uniquely identify the user so the cookie owner can track the user as he or she

moves around the internet—whether on the cookie owner's website or not. Facebook uses this type of third-party cookie when Facebook account holders use the Facebook app or website. As a result, when a Facebook account holder uses Defendants' Website, a unique id is sent to Facebook along with the intercepted communication that allows Facebook to identify the patient associated with the Private Information it has intercepted.

70. Furthermore, if the patient is also a Facebook user, the information Facebook receives is linked to the patient's Facebook profile (via their FID), which includes other identifying information.

71. Defendants intentionally configured the Pixels installed on their Website to capture both the "characteristics" of individual patients' communications with the Defendants' Websites (*i.e.,* their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (*i.e.*, the buttons, links, pages, and tabs they click and view).

72. As an example, anyone who visits one of Defendants' websites, such as *https://rayusradiology.com/*, and clicks on the "Services" tab is presented with an extensive list of various links to pages with information on specific conditions, treatments, services, and locations, ranging from "Bone Density" testing to "EKG[s]." Someone who clicks on the "Varicose and Spider Vein Treatment" button is directed to a page, *https://rayusradiology.com/services/interventional-and-vascular/varicose-and-spider-vein-treatment/*, which includes buttons and links that allow patients to schedule free vein screening appointments and provide information about specific conditions, risk factors, treatment options, services, locations, and a menu of frequently asked questions, each with

a separate link. Selecting any of these links, like "How Do I Know If I Need Vein Treatment?," directs them to a new page, *https://rayusradiology.com/services/interventional-and-vascular/varicose-and-spider-vein-treatment/#how-do-i-know-if-i-need-vein-treatment*, providing more information about vein treatments, signs a person may need treatment, and common issues that arise when varicose veins go untreated.

73. The Facebook Pixel intercepts the "characteristics" and "content" of all these communications with Defendants' Website, and automatically transmits this data to Facebook. Thus, by receiving the contents of these communications, Facebook will know the exact webpages that a specific patient has viewed and buttons clicked on, which relates to the patient's past, present, or future health conditions (*i.e.*, the patient's individually-identifiable patient health information).

74. As another example, when a patient visits the *https://rayusradiology.com/* homepage, navigates to the search bar, and types in specific search terms, that information is shared with Facebook through the Pixel in the form of full string URLs. Thus, on information and belief, if a patient types in "Lung Cancer Screening" into the search bar, when the webpage loads into the patient's browser, the Pixel code is triggered, which secretly sends an HTTP Request to Facebook including the patient's FID and the URL, informing Facebook that the user is searching for information on lung cancer screening by transmitting the following URL to Facebook: https://rayusradiology.com/?s=Lung+Cancer+Screening.

75. Upon information and belief, when patients click the "Patient Portal" button on Defendants' Website, which directs a patient to Defendants' patient portal login page, the Tracking Pixel similarly intercepts and records the patient's request to log into their confidential patient portal.

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

77. Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."[26] Thus, the communications between patients and Defendants, which are necessary to use Defendants' Online Platforms, are actually received by Defendants and stored on their server before Conversions API collects and sends the Private Information contained in those communications directly from Defendants to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

[26] *Prepare Your Business to Use the Conversions API*, FACEBOOK, https://www.facebook.com/business/help/1295064530841207?id=818859032317965 (last visited Mar. 21, 2023).

78. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the host server, companies like Facebook instruct Defendants to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendants "to share website events [with Facebook] that the pixel may lose."[27] Thus, it is reasonable to infer that Facebook's customers who implement the Facebook Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround.

79. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content on the host website. In other words, Facebook and others like it are not providing anything to the user related to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner.

80. Thus, without any knowledge, authorization, or action by the user, website owners like Defendants can use their source code to commandeer their patients' computing devices, causing the devices' web browsers to contemporaneously and invisibly re-direct the patients' communications to hidden third parties.

81. In this case, Defendants employed just such a device to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to third parties like Facebook contemporaneously, invisibly, and without the patient's knowledge.

[27] *Best Practices for Conversions API*, FACEBOOK, https://www.facebook.com/business/help/308855623839366?id=%20818859032317965 (last visited Mar. 21, 2023).

82. Consequently, when Plaintiffs and Class Members visited Defendants' website and communicated their Private Information, including but not limited to, medical treatment sought, medical conditions, appointment type and date, specific button/menu selections, content (such as searches for symptoms or treatment options) typed into free text boxes, demographic information, email addresses, and phone numbers, it is simultaneously intercepted and transmitted to third parties like Facebook.

iii. Defendants Violated Their Own Privacy Policies

83. Rayus Radiology maintains a Privacy Policy which applies to Defendant Medical Scanning Consultants, P.A. d/b/a Center for Diagnostic Imaging d/b/a Rayus Radiology and its affiliates.[28]

84. Defendants' Privacy Policy provides:

> PURPOSE STATEMENT
>
> The Health Insurance Portability and Accountability Act ("HIPAA") requires Center for Diagnostic Imaging and their affiliates to maintain the privacy of an Individual's Protected Health Information ("PHI"), and to provide individuals with notice of its legal duties and privacy practices with respect to PHI, as well as individuals' rights regarding their PHI. The following defines RAYUS's privacy policy and practices:
>
> OUR DUTY TO SAFEGUARD YOUR PROTECTED HEALTH INFORMATION
>
> Individually identifiable information about your past, present, or future health or condition, or the provision of healthcare is considered "Protected Health Information" or "PHI". We are required to extend certain protections to your PHI. Except in specified circumstances, we must use or disclose only the minimum necessary PHI to accomplish our intended purpose. We are required to follow the privacy practices described in this Notice, but we

[28] *Privacy Policy*, RAYUS RADIOLOGY (May 11, 2015), https://rayusradiology.com/privacy-policy/.

> reserve the right to change our privacy practices and the terms of this Notice at any time. The revised Notice will be available from any Center for Diagnostic Imaging center and will also be posted on our Web site at https://rayusradiology.com.
>
> HOW WE MAY USE AND DISCLOSE YOUR PROTECTED HEALTH INFORMATION
>
> We use and disclose PHI for a variety of reasons. If we disclose your PHI to an outside entity in order for that entity to do something on our behalf, we must have in place an agreement from the outside entity that it will protect the privacy of your information to the same extent that we do. We have a limited right to use and/or disclose your PHI for purposes of treatment, payment and for our healthcare operations. For uses beyond that, we must have your written authorization (or permission) unless the law permits or requires us to make the use or disclosure without your authorization. The law provides that we are permitted to make some uses/disclosures without your consent or authorization. The following describes and offers examples of our potential uses/disclosures of your PHI.[29]

85. Defendants' Privacy Policy does not permit Defendants to use and disclose Plaintiffs' and Class Members' Private Information for marketing purposes without written permission.[30]

86. Defendants' Privacy Policy further states:

> USES AND DISCLOSURES OF PHI REQUIRING AUTHORIZATION
>
> For uses and disclosures for purposes other than treatment, payment and operations, we are required to have your written authorization, unless the use or disclosure falls within one of the exceptions described below. Most uses and disclosures of psychotherapy notes, uses and disclosures for marketing purposes, and disclosures that constitute the sale of PHI require your authorization. Authorizations can be revoked at any time to stop future uses/disclosures except to the extent that we have already relied on your authorization.[31]

[29] *Id.*
[30] *Id.*
[31] *Id.*

87. Further, Rayus Radiology's Website Terms of Use provides, "[t]he following terms and conditions (together with any documents referred to in them) . . . apply to your use of our website and any content, functionality and services offered at rayusradiology.com . . ., which is owned and operated by us."[32]

88. Defendants' Terms of Use specifically state:

> **Access**
> To communicate with us through the Site, you may be asked to provide certain information. You represent and warrant that all information provided by you is accurate and complete. **Our Privacy Policy (located here) describes the personal information we collect, use, manage, disclose, and share.** You may also communicate with us through blog comments, videos or other interactive content on the site. These Terms of Use dictate your conduct when interacting on our Site.[33]

89. Defendants' Privacy Policy makes no mention of Defendants' use of third-party tracking technologies, such as the Facebook Pixel, within its Online Platforms to passively and surreptitiously intercept and transmit confidential patient communications and Private Information to unauthorized entities such as Meta (Facebook) and other likely third parties.

90. Defendants violated their own Privacy Policy by unlawfully disclosing Plaintiffs' and Class Members' Private Information to Meta (Facebook) and likely other third parties. Defendants further misrepresented that they would preserve the confidentiality of Plaintiffs' and Class Members' Private Information and the anonymity of their identities.

---

[32] *Terms of Use*, *supra* note 12.
[33] *Id.* (emphasis added).

iv. Warnings about the Pixel's Interception and Transmission of Private Information and Defendants' Implementation of the Pixel

91. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[34] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

92. On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective . . . at preventing the receipt of sensitive data."[35]

93. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical

---

[34] Kurt Wagner, *Facebook admits another blunder with user data*, FORTUNE (July 1, 2020), https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.

[35] N.Y. STATE DEP'T OF FIN. SERVS., REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS 7–8 (2021), *available at* https://www.dfs.ny.gov/system/files/documents/ 2021/02/facebook_report_20210218.pdf.

data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[36] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[37]

94. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that, "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[38]

95. Furthermore, in June of 2022, The Markup, a nonprofit newsroom and media organization focusing on technology and its effects on society, conducted an investigation

[36] Justin Sherman, *Your Health Data Might Be for Sale*, SLATE (June 22, 2022), https://slate.com/technology/2022/06/health-data-brokers-privacy.html.
[37] *Id.*
[38] Lorenzo Franceschi-Bicchierai, *Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document*, VICE (Apr. 26, 2022), https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.

of the use of tracking tools, such as the Facebook Pixel, on the online platforms of Newsweek's top 100 hospitals in America.[39]

96. The investigation by The Markup revealed that the Facebook Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[40] On those hospital websites, the Facebook Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website by, for example, clicking a button to schedule a doctor's appointment.[41] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[42]

97. The Markup found that the data the Facebook Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[43]

98. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he

---

[39] Todd Feathers et al, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*

was "deeply troubled" by what the hospitals were doing by capturing patient data and sharing it.[44]

99. Despite knowing that the Facebook Pixel code embedded in its Online Platforms was sending patients' personal health information to Facebook, Defendants did nothing to protect their patients from egregious intrusions into their patients' privacy, choosing instead to benefit at those patients' expense.

100. An example illustrates the point. If a user visits Defendants' Website, enters a condition or service (such as "Carpal Tunnel Injection") into Defendants' Website's search field, and clicks the search button, the individual's browser sends a request to Defendants' server requesting that it load the search results webpage. Because Defendants utilize the Facebook Pixel, Facebook's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, causing the browser to secretly duplicate the communication with Defendants, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

101. Thus, along with the individual's Facebook ID, IP address, and other identifying information, Defendants also transmit that the user is seeking a carpal tunnel injection to Facebook and others that Defendants have configured their Pixel to interact with.

[44] *Id.*

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

103. Every time Defendants send a patient's website activity data to Facebook, that patient's PII is also disclosed, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to the corresponding Facebook profile and the person's real-world identity. A user who accesses Defendants' Online Platforms while logged into Facebook will transmit the user cookie to Facebook, which contains that user's unencrypted Facebook ID.

104. Google and other companies likewise process this data in a similar manner and use it to connect the information to particular individuals to build marketing and other data profiles.

105. Through the Pixel, Defendants share their patients' identities and online activity, including personal information and search results related to their private medical treatment.

106. Defendants could have configured their tracking software to limit the information that they communicated to third parties, but they did not and instead intentionally selected the features and functionality of the Pixel that resulted in the Disclosure.

107. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendants to disclose their Private Information or assist with intercepting their communications. Plaintiffs were never provided with any written notice that Defendants disclose their patients' protected health information, nor were they provided any means of opting out of such disclosures. Defendants nonetheless knowingly disclosed Plaintiffs' protected health information to Meta (Facebook) and other unauthorized entities.

108. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

109. By law, Plaintiffs are entitled to privacy in their protected health information and confidential communications. Defendants deprived Plaintiffs and Class Members of their privacy rights when they: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiffs' and Class Members' confidential communications, personally identifiable information, and protected health information; (2) disclosed patients' protected information to Facebook and others—unauthorized third-party eavesdroppers; and (3) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent.

B. Plaintiffs' Experiences

i. Plaintiff Robert Christensen's Experience

110. Plaintiff Christensen is a former patient of Defendants and received healthcare services from Rayus Radiology and physicians in their network. Plaintiff relied on Rayus Radiology's Online Platforms to communicate confidential patient information.

111. Plaintiff Christensen accessed Defendants' Online Platforms to receive healthcare services from Defendants at Defendants' direction and encouragement. Plaintiff reasonably expected that his online communications with Rayus Radiology were confidential, solely between himself and Rayus Radiology, and that such communications would not be transmitted to or intercepted by a third party.

112. Plaintiff Christensen is also a Facebook user.

113. Plaintiff Christensen provided his Private Information to Defendants and trusted that the information would be safeguarded according to Rayus Radiology's privacy policies and the law.

114. As described herein, Defendants sent Plaintiff Christensen's Private Information to Meta (Facebook) and others when he used Defendants' digital platforms to communicate healthcare and identifying information to Rayus Radiology.

115. On information and belief, via the Tracking Pixel and other technologies, Defendants sent to Facebook and other third parties Plaintiff Christensen's activities and confidential communications on Defendants' Website, including services he viewed, terms he searched for when viewing providers and treatment options, and appointment scheduling information.

116. Pursuant to the process described herein, Defendants assisted Meta (Facebook) and others with intercepting Plaintiff's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Defendants facilitated these interceptions without Plaintiff Christensen's knowledge, consent, or express written authorization.

117. By failing to receive the requisite consent, Defendants breached confidentiality and unlawfully disclosed Plaintiff Christensen's personally identifiable information and protected health information.

118. Since Plaintiff Christensen began using Defendants' Online Platforms, Plaintiff has received targeted medical advertising on social media, spam calls, and spam emails related to his medical treatment.

ii. Plaintiff Martha Russell's Experience

119. Plaintiff Russell is a current patient of Defendants and received healthcare services from Rayus Radiology and physicians in their network. Plaintiff Russell relied on Rayus Radiology's Online Platforms to communicate confidential patient information.

120. Plaintiff Russell accessed Defendants' Online Platforms to receive healthcare services from Defendants at Defendants' direction and encouragement. Plaintiff Russell reasonably expected that her online communications with Rayus Radiology were confidential, solely between herself and Rayus Radiology, and that such communications would not be transmitted to or intercepted by a third party.

121. Plaintiff Russell is also a Facebook user.

122. Plaintiff Russell provided her Private Information to Defendants and trusted that the information would be safeguarded according to Rayus Radiology's privacy policies and the law.

123. As described herein, Defendants sent Plaintiff Russell's Private Information to Meta (Facebook) and others when she used Defendants' digital platforms to communicate healthcare and identifying information to Rayus Radiology.

124. On information and belief, via the Tracking Pixel and other technologies, Defendants sent to Facebook and other third parties Plaintiff Russell's activities and confidential communications on Defendants' Website, including services she viewed and appointment scheduling information.

125. Pursuant to the process described herein, Defendants assisted Meta (Facebook) and others with intercepting Plaintiff Russell's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Defendants facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

126. By failing to receive the requisite consent, Defendants breached confidentiality and unlawfully disclosed Plaintiff Russell's personally identifiable information and protected health information.

127. Since Plaintiff Russell began using Defendants' digital healthcare platforms, Plaintiff has received targeted medical advertising on social media, spam calls, and spam emails related to her medical treatment.

C. Defendants Violated HIPAA Standards

128. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.[45]

129. Guidance from the United States Department of Health and Human Services ("HHS") instructs healthcare providers that patient status alone is protected by HIPAA.

130. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[46]

131. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."[47]

132. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse;" (2) "[r]elates to the past,

[45] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 165.508(a), 164.514(b)(2)(i).
[46] *The HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.
[47] 45 C.F.R. § 160.103.

present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."[48]

133. Under the HIPPA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination;" or (2)(i) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed: (A) Names; . . . (H) Medical record numbers; . . . (J) Account numbers; . . . (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; . . . and (R) [a]ny other unique identifying number, characteristic, or code . . . ; and (ii) [t]he covered entity must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."[49]

[48] *Id.*
[49] 45 C.F.R. § 160.514.

134. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization.[50]

135. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."[51] The statute states that a "person . . . shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization."[52]

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

137. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties.[53] There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm."[54] In such cases, the entity that knowingly obtains individually identifiable

[50] *Id.* §§ 160.103, 164.502.
[51] 42 U.S.C. § 1320d-6.
[52] *Id.*
[53] *Id.*
[54] *Id.*

health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both."[55]

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

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data . . . . If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[56]

139. In its guidance for Marketing, HHS further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.[57]

---

[55] *Id.*

[56] OFFICE OF CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION (2012), available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[57] OFFICE OF CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., MARKETING (2003), available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

140. 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.[58]

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.[59]

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers."[60]

141. In addition, the Office for Civil Rights (OCR) at HHS has issued a Bulletin (the "HHS Bulletin") to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies.[61]

142. The HHS Bulletin expressly provides,

> Tracking technologies are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications ("apps"). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity's health care operations. The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). Some regulated entities may share sensitive information with online tracking

[58] 65 Fed. Reg. 82717 (Dec. 28, 2000).
[59] 67 Fed. Reg. 53186 (Aug. 14, 2002).
[60] 78 Fed. Reg. 5642 (Jan. 25, 2013).
[61] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Mar. 21, 2023).

> technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures[62] of PHI to tracking technology vendors or any other violations of the HIPAA Rules. For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.[63]**

143. Tracking technology vendors like Facebook 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 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.[64]

144. The HHS Bulletin explained that, through tracking technologies such as the Facebook Pixel, covered entities disclose individual's information, including PHI,

---

[62] *See id.* at n.8 ("Regulated entities can use or disclose PHI, without an individual's written authorization, only as expressly permitted or required by the HIPAA Privacy Rule. *See* 45 CFR 164.502(a).").
[63] *Id.* (citations omitted) (emphasis added) (citing 45 C.F.R. § 164.508(a)(3); 45 C.F.R. § 164.501 (defining "Marketing")).
[64] *Id.*

provided when individuals use the entity's website or mobile applications, such as medical records numbers, addresses, appointment dates, person's IP addresses or location, medical device IDs or unique identifying codes.[65]

145. The Bulletin further explained that "[a]ll such IIHI [individually identifiable health information] 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 IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services."[66] This is because that information "connects the individual to the regulated entity . . . and thus relates to the individual's past, present, or future health or health care or payment for care."[67]

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

> Tracking on unauthenticated webpages
>
> [T]racking 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 tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal **… [and pages] that address[] specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances**. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available

[65] *Id.*
[66] *Id.*
[67] *Id.*

> appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.[68]

147. Ultimately, in the Bulletin, HHS made clear that covered entities, such as Defendants, must comply with HIPAA rules in connection with tracking technologies such as the Facebook Pixel, including but not limited to:[69]

- Ensuring that all disclosures of PHI to tracking technology vendors are specifically permitted by the Privacy Rule and that, unless an exception applies, only the minimum necessary PHI to achieve the intended purpose is disclosed.[33]

  - Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use.[34] However, the Privacy Rule does **not** permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI.[35]

  - If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individuals' HIPAA-compliant authorizations are required **before** the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do **not** constitute a valid HIPAA authorization.

  - Further, it is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.

148. As articulated in the HHS Bulletin, covered entities utilizing tracking technologies must also implement "administrative, physical, and technical safeguards" to protect transmitted PHI, such as appropriate encryption, authentication, and audit controls;

---

[68] *Id.* (emphasis added).
[69] *Id.*

and must notify affected individuals and others of any impressible disclosure of PHI to tracking technology vendors who compromise that PHI. "In such instances, there is a presumption that there has been a breach of unsecured PHI unless the regulated entity can demonstrate that there is a low probability that the PHI has been compromised."[70]

149. The HHS Bulletin further noted that the impermissible disclosure of PHI can cause myriad harm to individuals, including "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" and discloses highly-sensitive information regarding patients' diagnoses, and the nature, frequency and location of treatment.[71]

150. The Bulletin is not a pronouncement of new law, but instead reminded covered entities and business associates of their longstanding obligations under existing guidance. The HHS Bulletin cautioned that, "[w]hile it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI ***only*** as expressly permitted or required by the HIPAA Privacy Rule."[72]

151. In other words, HHS has expressly stated that Defendants have violated HIPAA Rules by implementing the Tracking Pixel.

---

[70] *Id.*
[71] *Id.*
[72] *Id.*

D. Defendants Violated Industry Standards

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

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

154. AMA Code of Ethics Opinion 3.1.1 provides:

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

155. AMA Code of Medical Ethics Opinion 3.2.4 provides:

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

156. AMA Code of Medical Ethics Opinion 3.2.2 provides:

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

E. Plaintiffs' and Class Members' Expectation of Privacy

157. Plaintiffs and Class Members were aware of Defendants' duty of confidentiality when they sought medical services from Defendants.

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

F. IP Addresses Are Personally Identifiable Information

159. On information and belief, through the use of the Tracking Pixels on Defendants' Website, Defendants also disclosed and otherwise assisted Facebook and other likely third parties with intercepting Plaintiffs' and Class Members' Computer IP addresses.

160. An IP address is a number that identifies the address of a devise connected to the Internet.

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

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

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

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

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

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses.[73]
- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information."[74]

166. Consequently, by disclosing IP addresses, Defendants' business practices violated HIPAA and industry privacy standards.

G. Defendants Were Enriched and Benefitted from the Use of the Pixel and Unauthorized Disclosures

167. The sole purpose of the use of the Tracking Pixel on Defendants' Website was marketing and profits.

168. In exchange for disclosing the Private Information of its patients, Defendants are compensated by third parties, like Facebook, in the form of enhancing advertising services and more cost-efficient marketing on its platform.

169. Retargeting is a form of online marketing that targets users with ads based on their pervious internet communications and interactions. Upon information and belief,

[73] *See* 45 C.F.R. § 164.514(2).
[74] 45 C.F.R. § 164.514(2)(ii); *see also* 45 C.F.R. § 164.514(b)(2)(i)(O).

as part of their marketing campaign, Defendants re-targeted patients and potential patients, including Plaintiffs and Class Members.

170. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendants.

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

171. Plaintiffs' data and Private Information has economic value, and Defendants' disclosure harmed Plaintiffs and the Class. Facebook regularly uses data that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences and then sells that information to advertising clients.

172. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

173. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it describes the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[75]

[75] Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, TIME (Jan. 9, 2017), https://time.com/4588104/medical-data-industry/.

174. 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."[76]

CLASS ACTION ALLEGATIONS

175. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of other similarly situated persons, as representative of the following Class and Subclasses:

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

> All persons residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Tracking Pixel and related technology on Defendants' Online Platforms.

177. The Texas Subclass that Plaintiff Robert Christensen seeks to represent is defined as follows:

> All persons residing in Texas whose Private Information was disclosed to a third party without authorization or consent through the Tracking Pixel and related technology on Defendants' Online Platforms.

178. The Tennessee Subclass that Plaintiff Martha Russell seeks to represent is defined as follows:

> All persons residing in Tennessee whose Private Information was disclosed to a third party without authorization or consent through the Tracking Pixel and related technology on Defendants' Online Platforms.

[76] Christina Farr, *Hospital Execs Say They are Getting Flooded with Requests for Your Health Data*, CNBC (Dec. 18, 2019), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

179. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers, directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, was well as their immediate family members.

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

181. **Numerosity:** The Members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Members of the Classes is unknown to Plaintiffs at this time, based on information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly accessed in the Disclosure, and each Class Member is apparently identifiable within Defendants' records.

182. **Commonality:** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include, without limitation:

a. Whether and to what extent Defendants had a duty to protect Plaintiffs' and Class Members' Private Information;

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

c. Whether Defendants had duties not to use Plaintiffs' and Class Members' Private Information for non-healthcare purposes;

d. Whether Defendants had duties not to use Plaintiffs' and Class Members' Private Information for unauthorized purposes;

e. Whether Defendants failed to adequately safeguard Plaintiffs' and Class Members' Private Information;

f. Whether and when Defendants actually learned of the Disclosure;

g. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

i. Whether Defendants failed to properly implement and configure the tracking software on their digital platforms to prevent the disclosure of information compromised in the Disclosure;

j. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Disclosure to occur; and

k. Whether Defendants engaged in unfair, unlawful, or deceptive practices by misrepresenting that they would safeguard Plaintiffs' and Class Members' Private Information.

183. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Disclosure, due to Defendants' use and incorporation of the tracking software.

184. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Classes in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Classes. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Classes, and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

185. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Members of the Classes and making final injunctive relief appropriate with respect to the Classes as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

186. **Predominance:** Defendants have engaged in a common course of conduct toward Plaintiffs and Members of the Classes, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out

above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

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

188. The nature of this action and the nature of laws available to Plaintiffs and Members of the Classes make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonable consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action

alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

189. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Members of the Classes demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

190. Adequate notice can be given to each Class Member directly using information maintained in Defendants' records.

191. Unless a Class-wide injunction is issued, Defendants may continue in their unlawful disclosure and failure to properly secure the Private Information of Members of the Classes, Defendants may continue to refuse to provide proper notification to Class Members regarding the Disclosure, and Defendants may continue to act unlawfully as set forth in this Complaint.

192. Furthermore, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Members of the Classes as a whole is appropriate.

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

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

b. Whether Defendants owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Disclosure;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Private Information; and

i. Whether Members of the Classes are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

CAUSES OF ACTION

COUNT I
Negligence
By All Plaintiffs Against Defendants

194. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

195. Defendants knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, misused, and disclosed to unauthorized parties.

196. As a provider of health care under the law, Defendants have a special relationship with Plaintiffs and Class Members who entrusted Defendants to adequately protect their Private Information.

197. Defendants knew that the Private Information at issue was private and confidential and should be protected as private and confidential, and thus, Defendants owed a duty of care not to subject Plaintiffs and Class Members to an unreasonable risk of unauthorized disclosure.

198. Defendants knew, or should have known, of the risks inherent in collecting and storing Private Information and allowing it to be accessed by unauthorized third parties.

199. Defendants' failure to take proper security measures to protect Plaintiffs' and Class Members' Private Information created conditions conducive to a foreseeable risk of unauthorized access and disclosure of Private Information to unauthorized third parties. As described above, Plaintiffs and Class Members are part of a foreseeable, discernable group that was at high risk of having their Private Information compromised, and otherwise wrongly disclosed if not adequately protected by Defendants.

200. Defendants had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

201. Defendants owed a duty to timely and adequately inform Plaintiffs and Class Members, in the event of their Private Information being improperly disclosed to unauthorized third parties.

202. Defendants systematically failed to provide adequate security for data in their possession or over which they had supervision and control.

203. Defendants, through their actions and omissions, unlawfully breached duties to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Defendants' possession, supervision, and control.

204. Defendants, through their actions and omissions, unlawfully breached duties owed to Plaintiffs and Class Members by failing to have appropriate procedures in place to prevent dissemination of Plaintiffs' and Class Members' Private Information.

205. Defendants, through their actions and omissions, unlawfully breached duties to timely and fully disclose to Plaintiffs and Class Members that the Private Information within Defendants' possession, supervision, and control was improperly accessed by unauthorized third parties, the nature of this access, and precisely the type of information improperly accessed.

206. Defendants' breach of duties owed to Plaintiffs and Class Members proximately caused Plaintiffs' and Class Members' Private Information to be compromised by being accessed by unauthorized third parties.

207. As a result, of Defendants' ongoing failure to adequately notify Plaintiffs and Class Members regarding what type of Private Information has been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages.

208. As a proximate result of Defendants' negligence and breach of duties as set forth above, Defendants' breaches of duty caused Plaintiffs and Class Members to, *inter alia*, have their data shared with third parties without their authorization or consent, receive unwanted advertisements that reveal seeking treatment for specific medical conditions, fear, anxiety and worry about the status of their Private Information, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over their Private Information, all of which can constitute actionable actual damages.

209. In failing to secure Plaintiffs' and Class Members' Private Information, Defendants are guilty of oppression, fraud, or malice. Defendants acted or failed to act with a reckless, willful, or conscious disregard of Plaintiffs' and Class Members' rights.

210. Defendants' conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class Members' Private Information, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Defendants' conduct. Plaintiffs and Class Members seek actual and compensatory damages and all other relief they may be entitled to as a proximate result of Defendants' negligence.

COUNT II
Negligence Per Se
By All Plaintiffs Against Defendants

211. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

212. Plaintiffs allege this negligence *per se* theory as alternative to their other negligence claims.

213. Pursuant to the laws set forth herein, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, Defendants were required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' Personal and Medical Information.

214. Plaintiffs and Class Members are within the class of persons that these statutes and rules were designed to protect.

215. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

216. Defendants owed a duty to timely and adequately inform Plaintiffs and Class Members, in the event of their Private Information being improperly disclosed to unauthorized third parties.

217. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party such as Facebook gaining access to Plaintiffs' and Class Members' Private Information, resulting in Defendants' liability under principles of negligence per se.

218. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information and not complying with applicable industry standards as described in detail herein.

219. Plaintiffs' and Class Member's Private Information constitute personal property that was taken and misused as a proximate result of Defendants' negligence, resulting in harm, injury and damages to Plaintiffs and Class Members.

220. As a proximate result of Defendants' negligence and breach of duties as set forth above, Defendants' breaches of duty caused Plaintiffs and Class Members to, *inter alia*, have their data shared with third parties without their authorization or consent, receive unwanted advertisements that reveal seeking treatment for specific medical conditions, fear, anxiety and worry about the status of their Private Information, diminution in the

value of their personal data for which there is a tangible value, and/or a loss of control over their Private Information, all of which can constitute actionable actual damages.

221. In failing to secure Plaintiffs' and Class Members' Private Information, Defendants are guilty of oppression, fraud, or malice. Defendants acted or failed to act with a reckless, willful, or conscious disregard of Plaintiffs' and Class Members' rights.

222. Defendants' conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class Members' Private Information, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Defendants' conduct. Plaintiffs and Class Members seek actual and compensatory damages and all other relief they may be entitled to as a proximate result of Defendants' negligence *per se.*

COUNT III
Invasion of Privacy – Publication of Private Facts
By All Plaintiffs Against Defendants

223. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

224. Plaintiffs' and Class Members' Private Information, including their communications with Defendants and sensitive data, are private facts that third parties, such as Facebook, acquired without the knowledge or consent of Plaintiffs and Class Members.

225. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendants via their Online Platforms.

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

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

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

229. Defendants allowed the public disclosure of Plaintiffs' and Class Members' Private Information to Meta (Facebook) and likely other third parties by allowing the Tracking Pixel and other tracking technologies to be used on their Online Platforms.

230. Defendants gave publicity to Plaintiffs' and Class Members' Private Information and the content of their communications by sharing them with unauthorized third parties. Many of those companies have business models predicated on building massive databases of individual consumer profiles from which to sell targeted advertising and make further disseminations.

231. Defendants' surreptitious tracking and commoditization of Plaintiffs' and Class Members' Private Information would be highly offensive to a reasonable person, particularly given that Defendants were their healthcare provider with whom they thought they were communicating confidential facts.

232. Plaintiffs and Class Members did not authorize, consent, know about, or take any action to indicate consent to Defendants' conduct alleged herein.

233. There is no legitimate public concern with respect to the Private Information of Plaintiffs and Class Members.

234. As a result of Defendants' public disclosure of Plaintiffs' and Class Members' Private Information, Plaintiffs and Class Members have been needlessly harmed by having their private and confidential medical information disseminated for profit by Defendants, Meta (Facebook) and likely other third parties.

235. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

236. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, restitution injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

COUNT IV
Invasion of Privacy – Intrusion Upon Seclusion
By All Plaintiffs Against Defendants

237. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

238. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendants via their Online Platforms.

239. Plaintiffs and Class Members communicated Private Information that they intended only for Defendants to receive and that they understood Defendants would keep private.

240. Defendants' disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiffs and Class Members is an intentional intrusion upon Plaintiffs' and Class Members' solitude or seclusion.

241. Plaintiffs and Class Members had a reasonable expectation that their communications, identity, health information, and other data would remain confidential and that Defendants would not install wiretaps, such as the Tracking Pixel, on their Online Platforms to secretly record and transmit their communications to unauthorized third parties.

242. As a direct and proximate result of Defendants' actions, Plaintiffs and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

243. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

244. Plaintiffs also seek such other relief as the Court may deem just and proper.

COUNT V
Breach of Implied Contract
By All Plaintiffs Against Defendants

245. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

246. Defendants solicited and invited Plaintiffs and Class Members to provide their Private Information through Defendants' Online Platforms as part of their regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

247. Defendants required Plaintiffs and Class Members to provide their Private Information, including full names, email addresses, phone numbers, computer IP addresses, appointment information, medical insurance information, medical provider information, medical histories, and other content submitted on Defendants' Website as a condition of their receiving healthcare services.

248. As a condition of utilizing Defendants' Online Platforms and receiving services from Defendants, Plaintiffs and Class Members provided their Private Information and compensation for their medical care. In so doing, Plaintiffs and Class Members entered into contracts with Defendants by which Defendants agreed to safeguard and protect such information, in its Privacy Practices and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

249. Implicit in the agreement between Defendants and their patients was the obligation that both parties would maintain the Private Information confidentially and securely.

250. Defendants had an implied duty of good faith to ensure that the Private Information of Plaintiffs and Class Members in their possession was used only as

authorized, such as to provide medical treatment, billing, and other medical benefits from Defendants.

251. Defendants had an implied duty to protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses.

252. Additionally, Defendants implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

253. Plaintiffs and Class members reasonable believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

254. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendants. Defendants did not. Plaintiffs and Class Members would not have provided their confidential Private Information to Defendants in the absence of their implied contracts with Defendants and would have instead retained the opportunity to control their Private Information for uses other than medical treatment, billing, and benefits from Defendants.

255. Consumers of medical services value their privacy and the ability to keep confidential their Private Information associated with obtaining such services. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants and entered into these implied contracts with Defendants without an understanding that their Private Information would be safeguarded and protected, nor would Plaintiffs and Class Members have entrusted their Private Information to Defendants in the absence of

Defendants' implied promise to monitor the Online Platforms, computer systems, and networks to ensure that reasonable data security measures were adopted and maintained.

256. Defendants breached the implied contracts with Plaintiffs and Class Members by disclosing Plaintiffs' and Class Members' Private Information to unauthorized third parties, failing to properly safeguard and protect Plaintiffs' and Class Members' Private Information; and violating industry standards as well as legal obligations that are necessarily incorporated into implied contract between Plaintiffs, Class Members, and Defendants.

257. The Disclosure was a reasonably foreseeable consequence of Defendants' actions in breach of the implied contracts.

258. Defendants' acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiffs and Class Members to provide their Personal Information in exchange for medical treatment and benefits.

259. As a result of Defendants' failure to fulfill the data security protections promised in these implied contracts, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value.

260. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiffs and Class Members have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities, the loss of control of their Private Information, disruption of their medical care and treatment, and the loss of the benefit of the bargain they had struck with Defendants.

261. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT VI
Unjust Enrichment
By All Plaintiffs Against Defendants

262. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

263. This claim is pleaded in the alternative to Plaintiffs' breach of implied contract claims.

264. Plaintiffs and Class Members conferred a monetary benefit upon Defendants in the form of valuable sensitive medical information that Defendants collected from Plaintiffs and Class Members under the guise of keeping this information private. Defendants collected, used, and disclosed this information for their own gain, including for advertisement purposes, sale, or trade for valuable services from third parties. Additionally, Plaintiffs and Class Members conferred a benefit on Defendants in the form of monetary compensation.

265. Plaintiffs and Class Members would not have used Defendants' services or would have paid less for those services if they had known that Defendants would collect, use, and disclose this information to third parties.

266. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members.

267. As a result of Defendants' conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

268. The benefits that Defendants derived from Plaintiffs and Class Members rightly belong to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles for Defendants to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

269. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds they received as a result of their conduct and the Disclosure alleged herein.

COUNT VII
Breach of Fiduciary Duty
By All Plaintiffs Against Defendants

270. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

271. A relationship existed between Plaintiffs and the Class on the one hand and Defendants on the other in which Plaintiffs and the Class put their trust in Defendants to protect the Private Information of Plaintiffs and the Class and Defendants accepted that trust.

272. Defendants breached the fiduciary duty that they owed to Plaintiffs and the Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, and intentionally disclosing, the Private Information of Plaintiffs and the Class.

273. Defendants' breach of fiduciary duty was a legal cause of damage to Plaintiffs and the Class.

274. But for Defendants' breach of fiduciary duty, the damage to Plaintiffs and the Class would not have occurred.

275. Defendants' breach of fiduciary duty contributed substantially to producing the damage to the Plaintiffs and the Class.

276. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiffs and Class Members are entitled to and do demand actual, consequential, and nominal damages, injunctive relief, and all other relief allowed by law.

COUNT VIII
Violation of the Texas Medical Practices Act
Tex. Occ. Code §§ 159.001, *et seq*.
By Plaintiff Robert Christensen
on Behalf of the Texas Subclass Against Defendants

277. The Texas Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Texas Subclass, re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

278. Under Tex. Occ. Code § 159.002(a)–(b), communications between a physician and a patient, relative to or in connection with any professional services as a physician to the patient, including records of the identity, diagnosis, evaluation, or

treatment of a patient by a physician that is created or maintained by a physician, are confidential and privileged.

279. Under Tex. Occ. Code § 159.002(c), a person, including a hospital or medical provider, that receives information from a confidential communication or record as described above and acts on the patient's behalf, may not disclose such information except to the extent that disclosure is consistent with the authorized purposes for which the information was first obtained.

280. Defendants' above-described wrongful actions, inaction and/or omissions that caused the Disclosure, caused the unauthorized disclosure of Plaintiff's and Class Members' Private Information, and caused Plaintiff and Class Members to suffer the resulting harm and damages collectively constitute the unauthorized release of confidential and privileged communications in violation of the Texas Medical Practice Act.

281. Plaintiff and Class Members, therefore, are entitled to injunctive relief and/or to recover their damages under Tex. Occ. Code § 159.009.

COUNT IX
Violation of Tennessee Consumer Protection Act of 1977 ("TCPA")
Tenn. Code Ann. §§ 47-18-109, *et seq.*
By Plaintiff Martha Russell
on Behalf of the Tennessee Subclass Against Defendants

282. The Tennessee Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

283. Defendants are "persons," as defined by Tenn. Code § 47-18-103(13).

284. Plaintiff and Tennessee Subclass Members are "consumers," as meant by Tenn. Code § 47-18-103(2).

285. Defendants advertised and sold "goods" or "services" in "consumer transaction[s]," as defined by Tenn. Code §§ 47-18-103(7), (18) & (19).

286. Defendants advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee, as defined by Tenn. Code §§ 47-18-103(7), (18) & (19). Defendants' acts or practices affected the conduct of trade or commerce, under Tenn. Code § 47-18-104.

287. Defendants violated the following provisions of Tenn. Code § 47-18- 104(b):

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

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

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

288. Defendants committed deceptive acts, including but not limited to encouraging patients to use Defendants' Online Platform while representing to patients that Defendants are committed to protecting the privacy and confidentiality of the Private Information patients provide. Defendants also promised patients that they would never sell patients' medical information without patients' written authorization.

289. Despite these representations, Defendants disclosed information relating to Plaintiff's and Class Members' medical treatment to third parties without their knowledge,

consent or authorization as part of a scheme, artifice or device with the intent to mislead patients.

290. Plaintiff and Class Members relied on Defendants' representations in using Defendants' Online Platform and thought they were communicating only with their trusted healthcare provider.

291. By installing and implementing Facebook's Pixel, Conversion API tools, and other tracking technologies, Defendants knew or reasonably should have known they intercepted and transmitted Plaintiff's and Class Member's communications from Plaintiff's and Class Members' browsers directly to Facebook and other third parties, or recorded on Defendants' servers and then transferred to Facebook via Conversions API.

292. Defendants' misleading, or otherwise false, claims regarding the confidentiality and security of patients' Private Information cause injuries to consumers, including Plaintiff and Class Members, and are unfair and deceptive because consumers do not receive services commensurate with the consumers' reasonable expectations.

293. Defendants' misleading, or otherwise false, claims regarding the confidentiality and security of patients' Private Information cause injuries to consumers, including Plaintiff and Class Members, and are unfair and deceptive because consumers end up overpaying for Defendants' services and receiving services of lesser standards than what they reasonably expected and bargained to receive.

294. Patients, such as Plaintiff and Class Members, cannot avoid any of these injuries caused by Defendants' deceptive representations regarding the confidentiality and security of patients' Private Information. Accordingly, the injuries Defendants caused

outweigh any possible benefit, if any exists, from the unauthorized disclosure of Plaintiff's and Class Members' Private Information.

295. Defendants' claims regarding the confidentiality and security of patients' Private Information are false, misleading, and unreasonable, and constitutes unfair and deceptive conduct. Defendants knew or should have known of their unfair and deceptive conduct.

296. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers. Defendants also intended to mislead Plaintiff and the Tennessee Subclass Members and to induce Plaintiff and the Tennessee Subclass Members to rely on their misrepresentations and omissions.

297. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Tennessee Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition, if any exist.

298. Defendants' "unfair" acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. Consumers could not have reasonably avoided injury because Defendants' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making, such as individual consumer analysis to determine whether Defendants would maintain and protect the confidentiality of patients' Private Information.

299. Defendants' misleading claims regarding the security and confidentiality of patients' Private Information had no countervailing benefit to consumers or to competition, or at least no benefit that outweighs the injury to consumers.

300. Defendants acted knowingly and its conduct present a continuing risk to Plaintiff and the Tennessee Subclass members.

301. Plaintiff and the Tennessee Subclass have suffered injury in fact and have lost money as a result of Defendants' unfair conduct. Plaintiff and the Class paid an unwarranted premium for Defendants' services, or otherwise bargained for services they did not receive. Specifically, Plaintiff and the Class paid for reasonable data security measures designed to protect their confidential PII and PHI from unauthorized disclosure; however, Defendants' data security practices failed to comply with federal and state law, industry standards, and Defendants' own representations.

302. Had Plaintiff and Class Members been aware that their Private Information would be transmitted to unauthorized third-parties, Plaintiff and Class Members would not have entered into transactions with Defendants and would not have provided payment or confidential medical information to Defendants.

303. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive trade practices, Plaintiff and Tennessee Subclass Members have suffered and will continue to suffer injury and damages.

304. Plaintiff and Tennessee Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorneys' fees.

COUNT X
Violation of the Tennessee Wiretapping and Electronic Surveillance Act
Tenn. Code Ann. § 39-13-601, *et seq.*
By Plaintiff Martha Russell
on Behalf of the Tennessee Subclass Against Defendants

305. The Tennessee Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

306. The Tennessee Wiretapping and Electronic Surveillance Act ("TWESA") states that it is a violation of the TWESA when a person:

(A) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(B) Intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

(i) The device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) The device transmits communications by radio, or interferes with the transmission of the communication;

(C) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection (a); or

(D) Intentionally uses, or endeavors to use, the contents of any wire, oral or electronic communication, knowing or having reason to know, that the information was obtained through the interception of a wire, oral or electronic communication in violation of this subsection (a).[77]

[77] TENN. CODE ANN. § 39-13-601(a).

307. Defendants intentionally intercepted, endeavored to intercept, or procured Plaintiff's and Class Members' electronic communications, without the consent of the Plaintiff and Class Members, using the Tracking Pixel and other tracking technologies.

308. Defendants intentionally intercepted, endeavored to intercept, or procured Plaintiff's and Class Members' electronic communications for the purpose of disclosing those communications to third parties, including Facebook, without the knowledge, consent, or written authorization of Plaintiff or Class Members.

309. Defendants intentionally disclosed or endeavored to disclose to Facebook and other unauthorized third parties the contents of Plaintiff's and Class Members' electronic communications, without the consent of Plaintiff and Class Members, using the Tracking Pixel and other tracking technologies.

310. Defendants intentionally used or endeavored to use Plaintiff's and Class Members electronic communications for the purpose of disclosing those communications to third parties, including Facebook, without the knowledge, consent, or written authorization of Plaintiff or Class Members.

311. Defendants knew or had reason to know that the contents of Plaintiff's and Class Members' electronic communications were obtained in violation of the TWESA through the use of the Tracking Pixel and other tracking technologies without the consent or written authorization of Plaintiff and Class Members.

312. Plaintiff's and Class Members' communications with Defendants constitute private conversations, communications, and information.

313. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendants via their Online Platforms.

314. Plaintiff and Class Members communicated sensitive PHI and PII that they intended for only Defendants to receive and that they understood Defendants would keep private.

315. Plaintiff and Class Members have a reasonable expectation that Defendants would not disclose PII, PHI, and confidential communications to third parties without Plaintiff's or Class Members' authorization, consent, or knowledge.

316. Plaintiff and Class Members had a reasonable expectation of privacy given Defendants' representations, Privacy Policy, Terms of Use, and HIPAA. Moreover, Plaintiff and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

317. Plaintiff and Class Members were unaware that their Private Information was being surreptitiously recorded and transmitted to third parties as they communicated with Defendants through their Online Platforms.

318. Without Plaintiff's or Class Members' knowledge, authorization, or consent, Defendants used the Tracking Pixel imbedded and concealed into the source code of their Online Platforms to secretly record and transmit Plaintiff's and Class Members' private communications to hidden third parties, such as Facebook.

319. The TWESA further provides, "[i]t is lawful . . . for a person not acting under color of law to intercept a wire, oral, or electronic communication, where the person is a party to the communication . . . , unless the communication is intercepted for the purpose

of committing any criminal or tortious act in violation of the constitution or laws of [Tennessee]."[78]

320. Defendants' purposes for intentionally intercepting and using the contents of Plaintiff's and Class Members' electronic communications were tortious in that Defendants disclosed Plaintiff's and Class Members protected and confidential Private Information to unauthorized third parties, invaded Plaintiff's and Class Members' privacy, and breached fiduciary duties to hold Plaintiff's and Class Members' Private Information securely and in confidence.

321. Under the TWESA, "any aggrieved person whose wire, oral or electronic communication is intentionally intercepted, disclosed, or used in violation of § 39-13-601 . . . may in civil action recover from the person or entity that engaged in that violation the following relief:"

(1) The greater of:

(A) The sum of the actual damages, including any damage to personal or business reputation or relationships, suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) Statutory damages of one hundred dollars ($100) a day for each day of violation or ten thousand dollars ($10,000), whichever is greater;

(2) Punitive damages; and

[78] TENN. CODE ANN. § 39-13-601(b)(5).

(3) A reasonable attorney's fee and other litigation costs reasonably incurred.[79]

322. Defendants are "persons" under the TWESA.[80]

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

a. Plaintiff's and Class Members' personal computing devices;

b. Plaintiff's and Class Members' web browsers;

c. Plaintiff's and Class Members browser-managed files;

d. Facebook's Pixel;

e. Internet cookies;

f. Defendants' computer servers;

g. Third-party source code utilized by Defendants; and

h. Computer servers of third parties (including Facebook) to which Plaintiff's and Class Members' communications were disclosed.

324. Defendants aided in the interception of communications between Plaintiff and Class Members and Defendants that were redirected to and recorded by third parties without Plaintiff's or Class Members' consent.

325. Under the TWESA, Plaintiff and the Class Members are entitled to recover actual damages and any profits made by Defendants as a result of Defendants' violations of the TWESA, but not less than statutory damages at a rate of $100 a day for each day of the violation or ten thousand dollars ($10,000), whichever is greater, reasonable attorney's fees, and court costs.

[79] TENN. CODE ANN. § 39-13-603(a).
[80] TENN. CODE ANN. § 39-11-106(30).

326. In addition to statutory damages, Defendants' breach caused Plaintiff and Class Members the following damages:

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

b. Defendants eroded the essential confidential nature of the doctor-patient relationship;

c. Defendants took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;

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

e. Defendants' actions diminished the value of Plaintiff's and Class Members' personal information.

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

COUNT XI
Violation of Minnesota Uniform Deceptive Trade Practices Act ("MDTPA")
Minn. Stat. §§ 325D.43, *et seq*.
By All Plaintiffs Against Defendants

328. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

329. Defendants advertised, offered, or sold goods or services in Minnesota and engaged in trade or commerce directly or indirectly affecting the people of Minnesota.

330. Defendants engaged in false, misleading, or deceptive acts and practices, in violation of the Minn. Stat. § 325D.44, including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that the person does not have;

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

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

d. Engaging in other conduct which similarly creates a likelihood of confusion or of misunderstanding.

331. Defendants committed deceptive acts, including but not limited to encouraging patients to use Defendants' Online Platform while representing to patients that Defendants are committed to protecting the privacy and confidentiality of the Private Information patients provide. Defendants also promised patients that they would never sell patients' medical information without patients' written authorization.

332. Despite these representations, Defendants disclosed information relating to Plaintiffs' and Class Members' medical treatment to third parties without their knowledge,

consent or authorization as part of a scheme, artifice or device with the intent to mislead patients.

333. Plaintiffs and Class Members relied on Defendants' representations in using Defendants' Online Platform and thought they were communicating only with their trusted healthcare provider.

334. By installing and implementing Facebook's Pixel, Conversion API tools, and other tracking technologies, Defendants knew or reasonably should have known they intercepted and transmitted Plaintiffs' and Class Member's communications from Plaintiffs' and Class Members' browsers directly to Facebook and other third parties, or recorded on Defendants' servers and then transferred to Facebook via Conversions API.

335. Defendants' misleading, or otherwise false, claims regarding the confidentiality and security of patients' Private Information cause injuries to consumers, including Plaintiffs and Class Members, and are unfair and deceptive because consumers do not receive services commensurate with the consumers' reasonable expectations.

336. Defendants' misleading, or otherwise false, claims regarding the confidentiality and security of patients' Private Information cause injuries to consumers, including Plaintiffs and Class Members, and are unfair and deceptive because consumers end up overpaying for Defendants' services and receiving services of lesser standards than what they reasonably expected and bargained to receive.

337. Patients, such as Plaintiffs and Class Members, cannot avoid any of these injuries caused by Defendants' deceptive representations regarding the confidentiality and security of patients' Private Information. Accordingly, the injuries Defendants caused

outweigh any possible benefit, if any exists, from the unauthorized disclosure of Plaintiffs' and Class Members' Private Information.

338. Defendants' claims regarding the confidentiality and security of patients' Private Information are false, misleading, and unreasonable, and constitutes unfair and deceptive conduct. Defendants knew or should have known of their unfair and deceptive conduct.

339. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers.

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

341. Plaintiffs and Class Members have suffered injury in fact and have lost money as a result of Defendants' unfair conduct. Plaintiffs and the Class paid an unwarranted premium for Defendants' services, or otherwise bargained for services they did not receive. Specifically, Plaintiffs and the Class paid for reasonable data security measures designed to protect their confidential PII and PHI from unauthorized disclosure; however, Defendants' data security practices failed to comply with federal and state law, industry standards, and Defendants' own representations.

342. Had Plaintiffs and Class Members been aware that their Private Information would be transmitted to unauthorized third-parties, Plaintiffs and Class Members would

not have entered into transactions with Defendants and would not have provided payment or confidential medical information to Defendants.

343. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive trade practices, Plaintiffs and Class Members have suffered and will continue to suffer the compromise and disclosure of their Private Information and identities, the loss of control of their Private Information, disruption of their medical care and treatment, lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Disclosure, the continued risk to their Private Information which remains in Defendants' possession, future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Disclosure, and overpayment for the services that were received without adequate data security.

344. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including an injunction barring Defendant from disclosing their Private Information without their consent; reasonable attorney's fees and costs; and any other relief that is just and proper.

COUNT XII
Violation of the Minnesota Consumer Fraud Act ("MCFA")
Minn. Stat. §§ 325F.69, *et seq.*
By All Plaintiffs Against Defendants

345. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

346. The Consumer Fraud Act prevents the "act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice."[81]

347. Defendants are "persons" as defined by Minn. Stat. § 325F.68.

348. Defendants committed false and deceptive acts, including but not limited to encouraging patients to use Defendants' Online Platforms while representing to patients that Defendants are committed to protecting the privacy and confidentiality of the Private Information patients provide. Defendants also promised patients that they would never sell patients' medical information without patients' written authorization.

349. Despite these representations, Defendants disclosed information relating to Plaintiffs' and Class Members' medical treatment to third parties without their knowledge, consent or authorization as part of a scheme, artifice or device with the intent to mislead patients.

350. Plaintiffs and Class Members relied on Defendants' representations in using Defendants' Online Platform and thought they were communicating only with their trusted healthcare provider.

351. By installing and implementing Facebook's Pixel, Conversion API tools, and other tracking technologies, Defendants knew or reasonably should have known they intercepted and transmitted Plaintiffs' and Class Member's communications from

[81] MINN. STAT. § 325F.69.

Plaintiffs' and Class Members' browsers directly to Facebook and other third parties, or recorded on Defendants' servers and then transferred to Facebook via Conversions API.

352. Plaintiffs have been damaged by this practice and are entitled to actual damages, injunctive relief, and reasonable attorneys' fees and costs.[82]

COUNT XIII
Violation of the Minnesota Health Records Act ("MHRA")
Minn. Stat. §§ 144.291 and 144.293
By All Plaintiffs Against Defendants

353. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

354. Under the Minnesota Health Records Act ("MHRA"), "health record" means any information, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of a patient; the provision of healthcare to a patient; or the past, present, or future payment for the provision of healthcare to a patient.[83]

355. The Private Information of Plaintiffs and the Class that was released in the Disclosure involved health records as that term is defined in the MHRA.

356. Plaintiffs and the Class are "patients" as that term is defined under the MHRA at all times relevant to this action under Minn. Stat. § 144.291, subd. 2(g).

357. Under the MHRA, it is unlawful for a third party to access a patient's health records from a provider, or a person who receives records from a provider, without the

[82] MINN. STAT. § 8.31(3a).
[83] MINN. STAT. § 144.291, subd. 2(c).

patient or the patient's legally authorized representative's consent, specific authorization in law, or a representative from a provider that holds a signed and dated consent from the patient authorizing the release.[84]

358. Via the Tracking Pixel and similar tracking technologies deployed on Defendants' Online Platforms, Defendants recorded and transmitted Plaintiffs' and the Class's health records to unauthorized third parties, such as Facebook and likely others.

359. Neither Plaintiffs nor the Class consented to have their health records released in the Disclosure.

360. Under the MHRA, a provider or other person who causes an unauthorized release of a health record by negligently releasing the health record is liable to the patient for compensatory damages, plus costs and reasonable attorney fees.[85] As a result of Defendants' violations of the MHRA, Plaintiffs and the Class Members seek all damages authorized by law, including compensatory damages plus costs, and reasonable attorney fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

[84] *Id.* § 144.293, subd. 2(1-3).

[85] *Id.* § 144.298, subd. 2.

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Disclosure;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e) Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of attorneys' fees and costs under the TCPA, TWESA, MDTPA, MCFA, MHRA, the common fund doctrine, and any other applicable law;

h) Costs and any other expense, including expert witness fees incurred by Plaintiffs in connection with this action;

i) Pre- and post-judgment interest on any amounts awarded; and,

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

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Respectfully submitted,

Dated: August 1, 2023

/s/ Brian C. Gudmundson

Brian C. Gudmundson (#336695)
Michael J. Laird (#398436)
Rachel K. Tack (#0399529)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Tyler B. Ewigleben*
Christopher D. Jennings*
Winston Hudson*
Laura Edmondson*
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300
Little Rock, AR 72201
Tel: (501) 372-1300
chris@yourattorney.com
tyler@yourattorney.com
winston@yourattorney.com
ledmondson@yourattorney.com

*To be admitted *pro hac vice*

Counsel for Plaintiffs and the Proposed Classes