MICHAEL KIND, ESQ.
Nevada Bar No.: 13903
KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123
Telephone: (702) 337-2322
Facsimile: (702) 329-5881
mk@kindlaw.com

David S. Almeida (*pro hac vice* anticipated)
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
708-529-5418
david@almeidalawgroup.com

Nicholas Migliaccio (*pro hac vice* anticipated)
Jason Rathod (*pro hac vice* anticipated)
Bryan G. Faubus (*pro hac vice* anticipated)
MIGLIACCIO & RATHOD LLP
412 H St. NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Attorneys For Plaintiffs & the Classes

CASE NO: A-24-906800-C
Department 17

DISTRICT COURT

CLARK COUNTY, NEVADA

W.M.F. and MATTHEW MARDEN, *individually and on behalf of all others similarly situated*,

Plaintiffs,

v.

LIFEMD, INC., a Delaware corporation,

Defendant.

Case No.: _____

Dept. No.: _____

CLASS COMPLAINT AND DEMAND FOR JURYT TRIAL

CLASS ACTION EXEMPT FROM ARBITRATION

Plaintiffs W.M.F. and Matthew Marden ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through undersigned counsel, hereby allege the following against Defendant LifeMD, Inc., which conducts business under the brand name REX MD (hereinafter, "REX MD" or "Defendant"). Facts pertaining to Plaintiffs and their personal experiences and circumstances are alleged based upon personal knowledge and all other facts set forth herein are alleged based upon the investigation of counsel and, where indicated, upon information and good faith belief.

INTRODUCTION

1. REX MD—a telehealth company that provides treatment options for several sensitive health conditions including cold sores, genital herpes, low testosterone, erectile dysfunction ("ED"), premature ejaculation and hair loss—purports to "take privacy and security seriously" and represents that it "complies with all relevant privacy and HIPAA regulations in the U.S."[1]

2. REX MD's privacy policies stated that "[u]nless [a user] affirmatively consent[s] and/or affirmatively opt[s]-in pursuant to an explicit request to do so, REX MD™ will never share, sell, rent, exchange or barter your personal information to or with any third-party for financial gain or marketing purposes,"[2] and, previously, that "any medical or health information that [a user] provide[s] that is subject to specific protections under applicable state laws (collectively, with [protected health information], "Protected Information"), will be used and disclosed only in accordance with such applicable laws."[3]

3. Those representations are ***not*** true as REX MD, in order to improve its advertising and increase its profits, made the conscious decision to install certain invisible tracking technologies on its website, https://rexmd.com/ (the "Website") in order to surreptitiously collect and disclose the individually identifiable health information ("IIHI") and protected health information ("PHI")

[1] *See* "About REX MD," available at https://rexmd.com/faq.php?affid=home&force=1 (last visited Nov. 21, 2024).

[2] *See* REX MD Privacy Policy Last Updated June 30, 2023, https://rexmd.com/privacy.php (last visited Nov. 21, 2024).

[3] *See* REX MD Privacy Policy, Date of last revision 9-09-19 (captured on Jan. 30, 2021), available at https://web.archive.org/web/20210130143713/https://rexmd.com/privacy.php (last visited Nov. 21, 2024).

(referred to herein collectively as "Private Information") of each and every visitor to and user of its Website ("Users" or "Class Members") to unauthorized third parties including, but not limited to, Meta Platforms, Inc. d/b/a Meta (referred to herein as "Facebook"), Google LLC and TikTok Inc. (collectively, the "Pixel Information Recipients").[4]

4. Invisible to the naked eye, the Pixels collect and transmit information from the User's browser to the corresponding Pixel Information Recipient as the user enters information into the Website. The Pixels secretly enable the unauthorized transmission and disclosure of Plaintiffs' and Class Members' Private Information by Defendant.

5. Upon information and good faith belief, Defendant also installed and implemented the Facebook Conversions Application Programming Interface ("Conversions API") on its servers. Conversions API serves the same purpose as the Facebook Pixel in that it surreptitiously collects and transmits Private Information to Facebook. Unlike the Pixels, however, Conversions API functions from Defendant's servers and therefore cannot be stymied by use of anti-Pixel software or other workarounds. Defendant secretly enabled additional unauthorized transmissions and disclosures of Plaintiffs' and Class Members' IIHI and PHI to Facebook by implementing the Conversions API.[5]

6. Through the use of the Pixels and Conversions API, Defendant's Website directs Plaintiffs' and Class Members' communications to automatically be sent to the servers of the corresponding Pixel Information Recipients. This collection and disclosure occurs on every webpage in which Defendant installed the Pixels and for which Defendant enabled Conversions API.[6]

7. Thus, operating as implemented by Defendant, the Pixels and Conversions API allow the Private Information that Plaintiffs and Class Members submit in confidence to be unlawfully

---

[4] Defendant's Website requires individuals to share highly sensitive Private Information in order to review available treatments for specific medical conditions, to create accounts, participate in highly sensitive and personal health screenings, and to receive treatment plans and order prescriptions.

[5] "Conversions API works with your Facebook Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Nov. 21, 2024).

[6] "Server events are linked to a dataset ID and are processed like events sent via the [Facebook] Pixel … This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." *See* https://developers.facebook.com/docs/marketing-api/conversions-api (last visited Nov. 21, 2024).

disclosed to the Pixel Information Recipients alongside the individual's unique personal identifiers, including his or her Facebook ID and/or other identifying information pertaining to any accounts they may have with any of the Pixel Information Recipients.[7]

8. Once Users' Private Information is collected and transmitted to, *e.g.*, Facebook, it is combined with a Users' Facebook profile and all of the information about this person is accessible via the User's unique Facebook ID ("FID").[8] The Pixel Information Recipients, in turn, use Plaintiffs' and Class Members' Private Information for business purposes, including using such information to improve advertisers' ability to target specific demographics and selling such information to third-party marketers who target Plaintiffs and Class Members online (*i.e.*, through their Facebook, Instagram, TikTok, and other social media and personal accounts).

9. The reason that REX MD went to these lengths to obtain this sensitive Private Information is, quite simply, because Plaintiffs' and Class Members would ***not*** provide it voluntarily; that is, if REX MD disclosed in its privacy policies that by using its Website a User's sensitive Private Information would be collected and disseminated to Facebook and/or other third-party platforms, no user would consent to that – or they would demand significant compensation for the use of their private and valuable health information in this manner.

10. To make matters worse, REX MD has ***not*** informed those Users of the disclosure of their Private Information as many other healthcare and telehealth entitles who have utilized similar tracking technology to collect and disclose Private Information to third parties have done.[9]

---

[7] Upon information and belief, Google and TikTok have their own mechanisms for matching received Private Information to specific individuals.

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

[9] In contrast to Defendant, in the last year, several medical providers that installed the Meta Pixel on their Web Properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf; Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies,* FIERCE HEALTHCARE (October 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-

11. This class action lawsuit is ***not*** a solution in search of a problem; rather, as the Federal Trade Commission and the Office for Civil Rights of the Department of Health and Human Services ("HHS") have reiterated the importance of and necessity for data security and privacy concerning health information. For instance, the FTC recently published a bulletin entitled *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases*, in which it noted that "[h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer's health***. Indeed, [recent FTC enforcement actions involving] *Premom*, *BetterHelp*, *GoodRx* and *Flo Health* ***make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or fertility, for example—or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information."***[10]

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

> ***Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.***
>
> In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.***
>
> [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that ***may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health***

aurora-health-data-breach-revealed-pixels-protected-health-information-3; *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWSWIRE (August 19, 2022), https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html.

[10] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases,* the FTC Business Blog (July 25, 2023) (emphasis added), *available at* https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Nov. 21, 2024).

information.[11]

13. Most recently, in July 2023, federal regulators sent a letter to approximately 130 healthcare providers warning them about the use of online tracking technologies that could result in unauthorized disclosures of Sensitive Information to third parties. The letter highlighted the "risks and concerns about the use of technologies, such as the Meta/Meta Pixel and Google Analytics, that can track a user's online activities," and warned about "[i]mpermissible disclosures of an individual's personal health information to third parties" that could "result in a wide range of harms to an individual or others." According to the letter, "[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more."[12]

14. The Office for Civil Rights ("OCR") at HHS has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (the "OCR Bulletin"), that the unlawful transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[13]

---

[11] *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization.

[12] *See* https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf (last visited Nov. 21, 2024).

[13] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html, HHS.GOV (emphasis added) (last visited Nov. 21, 2024) ("IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as in some circumstances IP addressor geographic location, does not include specific treatment or billing information like dates and types of health care services.").This guidance was recently vacated in part due to a court finding only part of it to be the product of improper rulemaking. *See American Hosp. Ass'n. v. Becerra,* 2024 WL 3075865 (S.D. Tex., Jun. 20, 2024). That Order found only that guidance regarding covered entities' collection and disclosure to third parties of users' IP addresses while they navigated unauthenticated public webpages ("UPWs") was improper. The Order in no way affects or undermines OCR's guidance regarding covered entities disclosing unique personal identifiers, such as Facebook identifiers, to third parties while patients make

15. The OCR Bulletin reminds healthcare organizations regulated under the HIPAA that they may use third-party tracking tools, such as Google Analytics or the Pixels *only in a limited way*, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.[14]

16. The OCR Bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.*** Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.*** While 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.***[15]

17. Despite these warnings from federal regulators, REX MD designed and maintained its Website so that Users would be required to submit Private Information in order to participate in health assessments and other health-related services, review treatments offered by Defendant for their medical conditions, purchase treatment options and create accounts, among many other things.

18. REX MD, in turn, put tracking technologies on its Wesbite that allowed third-party companies, such as Facebook, to intercept the Private Information to sell targeted advertising and/or otherwise monetize that information in the ever-growing marketplace for PII and PHI.

19. Despite the stigmas that unfortunately are so often associated with certain health issues

---

appointments for conditions, pay medical bills or log into (or use) a patient portal. *See id.* at 3-4, 31, n. 8 (vacating OCR guidance with respect to the "Proscribed Combination" defined as "circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a UPW addressing specific health conditions or healthcare providers" but stating "[s]uch vacatur is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane HHS document.").

[14] *See id*.

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

and treatments, Defendant intentionally chose to put its profits over the privacy of its users, which number several million.

20. Plaintiffs and Class Members provided their Private Information to Defendant by creating accounts, completing health assessments, researching doctors and other health-related services providers, reviewing conditions and available treatments, researching prescriptions, and/or purchasing subscription plans, making appointments, and, at all times throughout this process, had a reasonable expectation of privacy in the Private Information Defendant were collecting, including that Defendant would ensure that such Private Information remain secure and protected and only utilized for limited medical and health purposes.

21. Defendant owed common law, contractual, statutory and regulatory duties to keep Plaintiffs' and Class Members' Private Information safe, secure and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to patients to protect and safeguard their Private Information from unauthorized disclosure.

22. Defendant, however, failed in its obligations and promises by utilizing the Pixels and Conversions API on the Website as described herein, knowing that such technology would transmit and share Plaintiffs' and Class Members' Private Information with the Pixel Information Recipients.

23. While Defendant willfully and intentionally incorporated the Pixels and Conversions API into the Website, Defendant never disclosed to Plaintiffs or Class Members that it shared their Private Information, such as their sensitive and confidential assessment responses via the Website, with third parties. As a result, Plaintiffs and Class Members were unaware that their Private Information were being surreptitiously transmitted to the Pixel Information Recipients as they participated in health assessments and other health-related activities on Defendant's Website.

24. Defendant breached its obligations to Plaintiffs and the Class Members in one or more of the following ways: (i) failing to adequately review its 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 patients' Private Information; (iii) failing to obtain the consent of

patients, including Plaintiffs and Class Members, to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through the Pixels and Conversions API; (v) failing to warn Plaintiffs and Class Members of such sharing and disclosures; (vi) otherwise failing to design and monitor the Website to maintain the confidentiality and integrity of patients' Private Information.

25. Plaintiffs and Class Members have suffered injury because of Defendant's conduct. These injuries include (i) invasion of privacy, (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the transmissions of their Private Information to the Pixel Information Recipients, (iii) loss of the benefit of the bargain, (iv) diminution of value of the disclosed Private Information, (v) statutory damages and (vi) the continued and ongoing risk to their Private Information.

26. Plaintiffs seek to remedy these harms and therefore bring this class action lawsuit on behalf of similarly situated individuals whose sensitive Private Information was intentionally, recklessly and/or negligently disclosed to the Pixel Information Recipients through Defendant's unauthorized utilization of the Pixels, Conversions API and other similar tracking technologies. Plaintiffs assert individual and representative claims for: (i) negligence; (ii) invasion of privacy, (iii) breach of confidence; (iv) unjust enrichment; (v) violations of the Electronics Communication Privacy Act ("ECPA"), 18 U.S.C. § 2511(1); and (vi) violations of the Nevada Deceptive Trade Practices Act, NRS ch. 598.

PARTIES

A. Plaintiff W.M.F.

27. Plaintiff W.M.F. is, and at all relevant times was, a citizen of Las Vegas County, Nevada, where he intends to remain indefinitely.

28. In November 2020, Plaintiff W.M.F. accessed Defendant's Website on his personal electronic devices to research [redacted] and treatments for it, search for doctors and prescription medication and make appointments for his specific medical conditions.

29. In the process of using Defendant's services, Plaintiff W.M.F. was required to disclose

highly sensitive Private Information to Defendant. [redacted]

30. While Plaintiff W.M.F. was a user of Defendant's services, he never consented to or authorized the use of his Private Information by third parties or to Defendant enabling third parties to access, interpret and use such Private Information.

31. Plaintiff W.M.F. had an active Facebook account while he accessed Defendant's Website while logged into his Facebook account on the same device.

32. After using the Website, Plaintiff W.M.F. immediately began seeing targeted health ads related to his medical condition disclosed to Defendant, [redacted] as he scrolled through his social media accounts including Facebook.

B. Plaintiff Matthew Marden

33. Plaintiff Matthew Marden is, and at all relevant times was, a citizen of Marlborough County, Massachusetts, where he intends to remain indefinitely.

34. On multiple occasions beginning in or around 2016, Plaintiff Marden accessed Defendant's Website on his personal electronic devices to research his specific medical conditions and treatments for them, search for doctors and prescription medication.

35. In the process of using Defendant's services, Plaintiff Marden was required to disclose highly sensitive Private Information to Defendant. Specifically, Plaintiff Marden [redacted] and reviewed prices of prescriptions offered by Defendant for his medical condition.

36. While Plaintiff Marden was a user of Defendant's services, he never consented to or authorized the collection, disclosure or use of his Private Information.

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

38. After providing his Private Information to Defendant through the Website, Plaintiff Marden immediately began seeing targeted health ads related to his specific medical condition disclosed to Defendant, [redacted] as he scrolled through his social media accounts including Facebook.

C. Defendant

39. Defendant LifeMD, Inc. is a public corporation incorporated in Delaware and headquartered in New York County, New York.

40. Defendant LifeMD provides telehealth and other virtual healthcare services to patients across the country. These services include patient-provider audio/video meetings, lab testing, and prescriptions, and involve the solicitation of medical information from patients.

41. REX MD is a brand of Defendant's focusing on men's health that offers access to virtual medical treatment for a variety of men's health needs. Through REX MD's Website, Users can consult with an affiliated licensed physician and receive prescriptions from partner pharmacies.

42. Although REX MD initially launched in the ED treatment market, it now offers treatment for a variety of men's health conditions including premature ejaculation, testosterone and hair loss. As of December 31, 2022, REX MD has served more than approximately 390,000 customers and patients. [16]

JURISDICTION & VENUE

43. This Court has subject matter jurisdiction over this action under the NRS 14.065 because this Complaint asserts violations of Nevada law for which this Court's exercise of jurisdiction would violate neither the Nevada constitution nor the United States constitution. Plaintiffs and the Class seek damages in excess of $10,000.

44. This Court has personal jurisdiction over Defendant because Defendant is authorized to and regularly conducts business in the State of Nevada. Defendant contracts with clients within the State of Nevada and makes decisions impacting the privacy of said citizens' data and Private Information. These decisions include the use of Pixels, Conversions API, and other tracking technologies.

45. Venue is proper in this judicial district under NRS 13.010 because Defendant's contractual obligations were to be performed within this county. One or more plaintiffs reside within

[16] *Form 10-K*, LifeMD, Inc. (Dec. 31, 2022), https://www.sec.gov/ix?doc=/Archives/edgar/data/948320/000149315223008560/form10-k.htm#bs002 (last visited Nov. 21, 2024).

this county and contracted for and received Defendant's services within this county.

46. Therefore, the Eighth Judicial District Court, Clark County, Nevada has personal jurisdiction over both Plaintiffs and Defendants, and subject matter jurisdiction pursuant to Article 6, Section 6 of the Nevada Constitution and NRS 4.370

FACTUAL ALLEGATIONS

A. The Tracking Pixels

47. A "pixel" is a piece of code that "tracks the people and the types of actions they take"[17] as they interact with a website, including how long a person spends on a particular webpage, which buttons the person clicks, which pages they view, the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), and more.

48. Pixels are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting—*i.e.*, serving online advertisements to people who have previously engaged with a business's website—and other marketing.

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

50. The Pixels can also share the user's identifying information for easy tracking via the "cookies"[18] stored on their computer by any of the Pixel Information Recipients with which they have an account.

51. For example, Facebook stores or updates a Facebook-specific cookie every time a person accesses their Facebook account from the same web browser.

52. The Facebook Pixel can access this cookie and send certain identifying information like the user's Facebook ID to Facebook along with the other data relating to the user's Website inputs. The same is true for the other Pixel Information Recipients, which also create cookies that are stored

[17] RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Nov. 21, 2024).

[18] "Cookies are small files of information that a web server generates and sends to a web browser Cookies help inform websites about the user, enabling the websites to personalize the user experience." *See* https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Nov. 21, 2024).

in the user's computer and accessed by the Pixels to identify the user.

53. The Pixels are programmable, meaning that Defendant controls which of the webpages on the Website contain the Pixels, and which events are tracked and transmitted to the Pixel Information Recipients.

54. Defendant has utilized Pixels and other tracking technologies since at least January 2017.

55. Defendant used the data it collected from Plaintiffs and Class Members, without their consent, in an effort to improve its advertising and bolster its revenues.

B. Conversions API.

56. The Facebook Conversions API and similar tracking technologies allow businesses to send web events, such as clicks, form submissions, keystroke events, and other user actions performed by the user on the Website, from their own servers to Facebook and other third parties.[19]

57. Conversions API creates a direct and reliable connection between marketing data (such as a user's private and confidential actions on Defendant's Website) from Defendant's server to Facebook.[20] In doing so, Defendant stores Plaintiffs' and Class Members' Private Information on their own server and then transmits it to unauthorized third parties.

58. Conversions API is an alternative method of tracking versus the Facebook Pixel because no privacy protections on the user's end can defeat it. This is because it is "server-side" implementation of tracking technology, whereas the Pixels are "client-side," *i.e.*, executed on users' computers in their web browsers.

59. Because Conversions API is server-side, it cannot access the Facebook-specific cookie to retrieve the user's Facebook ID.21 Therefore, other roundabout methods of linking the user to their

---

[19] https://revealbot.com/blog/facebook-conversions-api/ (last visited Nov. 21, 2024).

[20] *See* https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Nov. 21, 2024).

[21] "Our systems are designed to not accept customer information that is unhashed Contact Information, unless noted below. Contact Information is information that personally identifies individuals, such as names, email addresses, and phone numbers, that we use for matching purposes only." *See* https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/ (last visited Nov. 21, 2024).

Facebook account are employed by Facebook.[22] For example, Facebook has an entire page within its developers' website about how to de-duplicate data received when both the Facebook Pixel and Conversions API are executed.[23]

60. Conversions API tracks the user's website interaction, including Private Information being shared, and then transmits this data to Facebook and other third parties. Facebook markets Conversions API as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."

61. Defendant installed the Pixels and Conversion API, as well as other tracking technologies, on many (if not all) of the webpages within the Website and programmed or permitted those webpages to surreptitiously share patients' private and protected communications with the Pixel Information Recipients—communications that included Plaintiffs' and Class Members' Private Information.

C. Defendant's Method of Transmitting Plaintiffs' & Class Members' Private Information via Pixel and Conversions API.

62. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as a computer, tablet, or smartphone) 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).

63. Every website is hosted by a computer "server" that holds the website's contents. The entity(ies) in charge of the website exchange communications with users' client devices as their web browsers query the server through the internet.

64. Web communications consist of Hypertext Transfer Protocol ("HTTP") or Hypertext

---

[22] "Sending additional customer information parameters may help increase Event Match Quality. Only matched events can be used for ads attribution and ad delivery optimization, and the higher the matching quality, the better." https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req- rec-params (last visited Nov. 21, 2024).

[23] *See* https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel-and-server-events (last visited Nov. 21, 2024).

Transfer Protocol Secure ("HTTPS") requests and HTTP or HTTPS responses, and any given browsing session may consist of thousands of individual HTTP requests and HTTP responses, along with corresponding cookies:

a. **HTTP request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (*i.e.*, web address), GET Requests can also send data to the host server embedded inside the URL and can include cookies. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF for filing a motion to a court).

b. **Cookies**: a small text file that can be used to store information on the client device that 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.

c. **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.

65. A patient's HTTP request essentially asks the Defendant's Website to retrieve certain information (such as a set of health screening questions). The HTTP response sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the participant's screen as they navigate Defendant's Website.

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

67. 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.

68. The Pixels are Source Code doing just that—surreptitiously transmitting a Website user's communications and inputs to the corresponding Pixel Information Recipient much like a traditional wiretap. When individuals visit Defendant's Website via an HTTP request to Defendant's server, Defendant's server sends an HTTP response (including the Markup) that displays the webpage visible to the user, along with Source Code (including the Pixels).

69. Thus, Defendant is, in essence, handing its patients a tapped phone and, once the webpage is loaded into the patient's browser, the software-based wiretaps are quietly waiting for private communications on the webpage to trigger the Pixels, which then intercept those communications intended only for Defendant and transmits those communications to the corresponding Pixel Information Recipient.

70. Third parties like the Pixel Information Recipients place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the user associated with the information intercepted (in this case, highly sensitive Private Information).

71. Defendant intentionally configured Pixels installed on its Website to capture both the "characteristics" of individual patients' communications with the Defendant's 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. Defendant also deposits cookies named _fbp, _ga_, and _gid onto Plaintiffs' and Class Members' computing devices. These are cookies associated with the third-parties Facebook and Google but which Defendant deposits on Plaintiffs' and Class Members' computing devices by disguising them as first-party cookies. And without any action or authorization, Defendant commands Plaintiffs' and Class Members' computing devices to contemporaneously re-direct the Plaintiffs' and Class Members' identifiers and the content of their communications to Facebook and Google.

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

74. Furthermore, if the patient is also a Facebook user, the information Facebook receives is linked to the patient's Facebook profile (via their Facebook ID or "c_user id"), which includes other identifying information.

D. Facebook's Platform & its Business Tools.

75. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[24]

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

77. Facebook's Business Tools, including the Facebook Pixel, 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.

78. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[25]

79. Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[26]

80. One such Business Tool is the Facebook Pixel, which "tracks the people and type of actions they take" on a webpage in which the Pixel has been installed.[27]

81. When a user accesses a webpage that is hosting the Facebook Pixel, their

---

[24] META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 21, 2024).

[25] *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Nov. 21, 2024); *see* META PIXEL, GUIDES, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/ (last visited Nov. 21, 2024); *see also* BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142 (last visited Nov. 21, 2024); META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Nov. 21, 2024).

[26] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142, FACEBOOK. COM (last visited Nov. 21, 2024); *see also* META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[27] RETARGETING, https://www.facebook.com/business/goals/retargeting, FACEBOOK. COM (last visited Nov. 21, 2024).

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

82. This second, secret transmission contains the original GET 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 Defendant's Website—Defendant's own code and Facebook's embedded code.

83. 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 Defendant's Website, including not only their medical searches, treatment requests, and the webpages they view, but also their unique personal identifiers including email address and/or phone number.

84. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[28] 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.

85. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. When 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. Likewise, Facebook maintains "shadow profiles" on users without Facebook accounts and links the information collected via the Facebook Pixel to the user's real-world identity using their shadow profile.[29]

86. A user's Facebook ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests,

---

[28] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited November 21, 2024).

[29] *See* Russell Brandom, *Shadow Profiles Are The Biggest Flaw In Facebook's Privacy Defense*, TheVerge.com (Apr 11, 2018), *available at* https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (last visited Nov. 21, 2024).

work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

87. The Private Information disclosed via the Pixel allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought. Facebook then uses that information to sell advertising to Defendant and other advertisers and/or sells that information to marketers who will online target Plaintiffs and Class Members.

88. With substantial work and technical know-how, internet users can sometimes circumvent the browser-based wiretap technology of the Pixels. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that even savvy users cannot evade. Facebook's workaround is called Conversions API.

89. Conversions API is effective because it transmits directly from the host server and does not rely on the user's web browser.

90. Thus, the communications between patients and Defendant, which are necessary to achieve the purpose of Defendant's Website, are received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.[30]

91. The Pixel Information Recipients track user data and communications for their own marketing purposes and for the marketing purposes of the website owner. Ultimately, the purpose of collecting user data is to make money.

---

[30]Although prior to discovery there is no way to confirm that Defendant has implemented Conversions API or another workaround (as that would require accessing the host server), Facebook instructs website owners like Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose." *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last accessed Nov. 21, 2024). Thus, it is reasonable to infer that Defendant is utilizing the Conversions API workaround.

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

93. In this case, Defendant employed the Pixels and Conversions API, among other tracking technologies, to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to Facebook and the other Pixel Information Recipients.

94. In sum, the Pixels and other tracking technologies on the Website transmitted Plaintiffs' and Class Members' highly sensitive communications and Private Information to the corresponding Pixel Information Recipient, which communications contained private and confidential medical information.

95. These transmissions were performed without Plaintiffs' or Class Members' knowledge, consent, or express written authorization.

E. Defendant's Use of the Pixels Violated Its Own Privacy Policies.

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

97. Defendant did not inform Plaintiffs that it shared their Private Information with Facebook and the other Pixel Information Recipients. Moreover, REX MD's Privacy and Personal Information Policy between September 9, 2019, and February 26, 2021 (the "2019 Privacy Policy"), does ***not*** explain that user and patient Private Information will be shared with Facebook or other unauthorized third parties.

98. In fact, the 2019 Privacy Policy expressly states the opposite:

> REX MD . . . automatically receives and records high tech non-personal information on our server logs from your browser including your IP address, cookie information and the page you requested. REX MD may use this information to customize the information, advertising and content you see and to fulfill your requests for certain products and services; with the ultimategoal [*sic*] to ensure your shopping experience is of the highest quality. **You can be assured, REX MD does not connect this non-**

personal data to any personal information collected from you.[31]

99. At best, this assurance is misleading.

100. The Pixels do, in fact, allow the Pixel Information Recipients to link "non-personal data" such as IP addresses and cookie information to personal information entered into Defendant's Website by patients.

101. Furthermore, Defendant's 2019 Privacy Policy claims that the information entered into the Website by a patient is "protected for your privacy and security," and that Defendant "safeguard[s] your personal information from unauthorized access, through access control procedures, network firewalls and physical security measures."[32]

102. The 2019 Privacy Policy does acknowledge that:

> REX MD may disclose your personal information to sister sites REX MD who workon [*sic*] behalf of REX MD to provide complementary products and services requested by you. **We will share personal information for these purposes only** as our sister sites REX MD [*sic*] have privacy policies that mirror ours or who agree to abide by our collective policies with respect to personal information.[33]

103. This section continues by listing four circumstances in which "REX MD may otherwise disclose your personal information," including with "express consent to share the information for a specified purpose."[34]

104. None of the four purposes listed circumstances cover Defendant's actions here, i.e., sharing the Private Information of Plaintiffs and the Class Members with the Pixel Information Recipients for business purposes.

105. Elsewhere in the 2019 Privacy Policy, REX MD acknowledges its use of third-party

---

[31] *REX MD Privacy and Personal Information Policy* (Sept. 9, 2019), *available at* https://web.archive.org/web/20210130143713/https://rexmd.com/privacy.php; *compare with REX MD Privacy and Personal Information Policy* (Feb. 26, 2021), *available at* https://web.archive.org/web/20210307045003/https://rexmd.com/privacy.php (last visited Nov. 21, 2024).

[32] *REX MD Privacy and Personal Information Policy* (Sept. 9, 2019), https://web.archive.org/web/20210130143713/https://rexmd.com/privacy.php (last visited Nov. 21, 2024).

[33] *Id.*

[34] *Id.*

vendors to conduct remarketing, but it does not disclose that this process involves the wholesale sharing of Plaintiffs' and the Class Members' Private Information:

> REX MD has implemented display advertising and uses remarketing with Google analytics to communicate and advertise online. It means that third-party vendors, including Google, show our ads on sites across the Internet to ensure you stay informed of our latest specials and products of interest.
> REX MD along with third-party vendors, including Google, use first-party cookies (such as the Google Analytics cookie) and third-party cookies (such as the DoubleClick cookie) together to inform, optimize, and serve ads based on your past visits to our website. This is typical with your other website browsing activities.[35]

106. This description of remarketing is misleading, especially in context, alongside the assurances discussed above.

107. In its Privacy Policy Defendant also takes the untenable and unsupported position that HIPAA does not apply to a user's basic personal information, stating that "your name, email address, shipping address and phone number . . . we do not consider to be 'protected health information' or 'medical information.'"[36]

108. The Privacy Policy further states "any information that does not constitute Protected Information under applicable laws may be used or disclosed in any manner permitted under this Privacy Policy."[37] As discussed above, this information is clearly protected by the HIPAA Privacy Rule.

109. REX MD's cavalier attitude towards patient information appears to stem from its mistaken belief that HIPAA does not apply to it. To wit, its Privacy Policy states that "REX MD is not a 'covered entity' under" HIPAA, explaining that "[i]t is important to note that HIPAA does not necessarily apply to an entity or person simply because there is health information involved, and

---

[35] *Id.*

[36] *See REX MD Privacy and Personal Information Policy* (Sept. 9, 2019), *available at* https://web.archive.org/web/20210130143713/https://rexmd.com/privacy.php; *REX MD Privacy and Personal Information Policy* (Feb. 26, 2021), available at https://web.archive.org/web/20210307045003/https://rexmd.com/privacy.php (last visited Nov. 21, 2024); *REX MD Privacy and Personal Information Policy* (Jun. 30, 2023), available at https://rexmd.com/privacy.php.

[37] *See id.*

HIPAA may not apply to your transactions or communications with REX MD, the Medical Groups, the Providers or the Pharmacies."[38]

110. Nevertheless, the Privacy Policy also acknowledges that REX MD "may be subject to certain provisions of HIPAA with respect to "protected health information" provided by patients to affiliated covered entities "[t]o the extent REX MD is deemed a "business associate" [of a covered entity], and solely in its role as a business associate."[39]

111. Defendant's equivocation is not a valid legal analysis—ultimately, REX MD is subject to HIPAA and failed to abide by the HIPAA Privacy Rule in implementing the Pixels and related tracking technologies on its Website.

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

113. As a "redundant" measure to ensure Plaintiffs' and Class Members' Private Information was successfully transmitted to third parties like Facebook, Defendant also implemented server-based workarounds like Conversions API to send Plaintiffs' and Class Members' Private Information from electronic storage on Defendant's server directly to Facebook, at a minimum.

F. Defendant's Use of the Pixels Violates HIPAA.

114. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.40

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

116. HIPAA's Privacy Rule defines "individually identifiable health information" as "a

---

[38] *Id.*

[39] *Id.*

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

subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

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

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

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

45 C.F.R. § 164.514.

119. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of PHI without authorization. 45 C.F.R. §§ 160.103, 164.502.

120. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be PHI.

121. The Department of Health and Human Services has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data, "[i]f 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."[41]

122. Consistent with this restriction, the HHS has issued marketing guidance that provides, "[w]ith limited exceptions, the [Privacy] 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 or enrollees to third parties without obtaining authorization from each person on the list."[42]

123. Here, as described, *supra*, Defendant provided patient information to third parties in violation of the Privacy Rule – and its own Privacy Policy.

124. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(c), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1) – which Defendant failed to do.

125. Defendant further failed to comply with other HIPAA safeguard regulations as follows:

a. Failing to ensure the confidentiality and integrity of electronic PHI that Defendant created, received, maintained, and transmitted in violation of 45

[41] *See Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited Nov. 21, 2024).

[42] *Marketing*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html, HHS.GOV (last visited Nov. 21, 2024).

C.F.R. section 164.306(a)(1);

b. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);

c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendant in violation ofc45 C.F.R. section 164.308(a)(6)(ii);

d. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. section 164.306(a)(2);

e. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3) and

f. Failing to design, implement, and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

126. Commenting on a June 2022 report discussing the use of Pixels by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it … It is quite likely a HIPAA violation."[43]

127. Defendant's use of third-party tracking code on its Website is a violation of Plaintiffs' and Class Members' privacy rights under federal law. While Plaintiffs do not bring a claim under HIPAA itself, this violation demonstrates Defendant's wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

G. Defendant Violated Industry Standards.

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

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

130. 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

[43] '*Deeply Troubled*': *Security experts worry about Facebook trackers on hospital sites*, ADVISORY BOARD, https://www.advisory.com/daily-briefing/2022/06/17/data-trackers (last visited Nov. 21, 2024).

> aspects, including, … personal data (informational privacy)[.]

131. AMA Code of Medical Ethics Opinion 3.2.4 provides:

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

132. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must: (c) Release patient information only in keeping ethics guidelines for confidentiality.[44]

133. Defendant's use of the Pixels also violates data security guidelines. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

134. The FTC's October 2016 publication *Protecting Personal Information: A Guide for Business*[45] established cyber-security guidelines for businesses. These guidelines state that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network vulnerabilities; and implement policies to correct any security problems.

135. As discussed herein, the FTC has since also made clear that healthcare companies should not use tracking technologies to collect sensitive health information and disclose it for marketing and advertising purposes without consumers' informed consent.[46]

---

[44] AMA Principles of Medical Ethics: I, IV, *Chapter 3: Opinions on Privacy, Confidentiality & Medical Records*, https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf, American Medical Association (last visited Nov. 21, 2024).

[45] Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 21, 2024).

[46] *See* note 10, *supra*.

136. In fact, as also described above, the FTC has recently brought enforcement actions against several healthcare companies, including Premom, BetterHelp, GoodRx and Flow Health for conveying information – or enabling an inference – about their consumers' health to unauthorized third parties without the consumers' consent.

137. Just like the telehealth companies fined by the FTC in recent years, Defendant failed to implement these basic, industry-wide data security practices.

H. Users' Reasonable Expectation of Privacy.

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

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

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

141. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[47]

142. Personal data privacy and obtaining consent to share Private Information are material to Plaintiffs and Class Members.

I. IP Addresses are Protected Health Information.

143. While not all health data is covered under HIPAA, the law specifically applies to

[47] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/, CONSUMERREPORTS.ORG (last visited Nov. 21, 2024).

healthcare providers, health insurance providers and healthcare data clearinghouses.[48]

144. One of the primary arguments that hospitals, telehealth companies and other disclosing entities have trotted out in defense of these "shocking" practices is that the information surreptitiously collected and disclosed is *not* PHI because it is all anonymized.[49]

145. Indeed, some healthcare providers claimed that the information collected from their websites was not personally identifiable because it was hashed; HIPAA allows health information to be shared when it has been de-identified. However, hashing does not anonymize data for the tech platforms that receive it and match it to user profiles.

146. And every data packet sent by a tech company's tracker includes the user's IP address, which is one of several unique identifiers that explicitly qualify health data for protection under HIPAA.[50]

147. Defendant improperly disclosed Plaintiffs' and Class Members' computer IP addresses to the Pixel Information Recipients through their use of the Pixels *in addition to* unique personal identifiers such as phone numbers, email addresses, dates of birth, Defendant's client ID numbers, services selected, assessment responses, patient statuses, medical conditions, treatments, provider information, and appointment information.

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

---

[48] *See* Alfred Ng & Simon Fondrie-Teitler, *This Children's Hospital Network Was Giving Kids' Information to Facebook* (June 21, 2022), available at https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook (last visited November 21,, 2024) (stating that "[w]hen you are going to a covered entity's website, and you're entering information related to scheduling an appointment, including your actual name, and potentially other identifying characteristics related to your medical condition, there's a strong possibility that HIPAA is going to apply in those situations").

[49] At a recent hearing, presiding judge in the *In re Facebook Pixel Tracking* case, the Honorable William H. Orrick, stated that "I think that is a kind of thing that a reasonable Facebook user would be shocked to realize" and "[i]f what the plaintiffs are saying is true … I think it's a big problem that there's not a specific consent."

[50] Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, *"Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies: An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech's tracking tools*, MARKUP (Dec. 13, 2022), available at https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies (last visited November 21, 2024).

Internet.

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

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

151. Facebook tracks every IP address ever associated with a Facebook user (and with non-users through shadow profiles). Google also tracks IP addresses associated with Internet users.

152. Facebook, Google, and other third-party marketing companies track IP addresses for targeting individual homes and their occupants with advertising.

153. Under HIPAA, an IP address is considered personally identifiable information, defining personally identifiable information as including "any unique identifying number, characteristic or code" and specifically listing IP addresses among examples. 45 C.F.R. § 164.514 (2).

154. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); see also, 45 C.F.R. § 164.514(b)(2)(i)(O).

155. Consequently, Defendant's disclosure of Plaintiffs' and Class Members' IP addresses violated HIPAA and industry-wide privacy standards.

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

156. The purpose of the use of the Pixels and other tracking technologies on Defendant's Website was to improve marketing and thereby boost revenues.

157. In exchange for disclosing the Private Information of their accountholders and patients, Defendant is compensated by the Pixel Information Recipients in the form of enhanced advertising services and more cost-efficient marketing on their platform.

158. Defendant was advertising their services through Facebook, for one, and the Pixels were used to "help [Defendant] understand which types of ads and platforms are getting the most

engagement[.]"[51]

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

160. Defendant retargeted patients and potential patients to get more people to use their services. These patients include Plaintiffs and Class Members.

161. Thus, utilizing the Pixels benefits Defendant by, among other things, reducing the cost of advertising and retargeting.

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

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

164. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[52]

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

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

---

[51] RETARGETING, https://www.facebook.com/business/goals/retargeting, FACEBOOK. COM (last visited Nov. 21, 2024).

[52] *See* https://time.com/4588104/medical-data-industry/ (last visited Nov. 21, 2024).

[53] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Nov. 21, 2024).

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

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

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

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

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

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

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

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

---

[54] *Id.*

[55] Federal Trade Commission, Warning Signs of Identity Theft, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Nov. 21, 2024).

[56] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited Nov. 21, 2024).

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

175. Defendant gave away Plaintiffs' and Class Members' Private Information without permission.

176. The unauthorized access to Plaintiffs' and Class Members' private and Personal Information has diminished the value of that information, resulting in harm to Website users, including Plaintiffs and Class Members.

177. Plaintiffs suffered damages in the form of (a) invasion of privacy; (b) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the invasion of privacy; (c) diminution of value of the Private Information; (d) statutory damages; (e) the continued and ongoing risk to their Private Information; (f) lost benefit of the bargain; and (g) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiffs' medical conditions and other confidential information they communicated to Defendant via the Website.

178. Plaintiffs have a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

TOLLING

179. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know—and had no way of knowing—that their Private Information was intercepted and unlawfully disclosed to the Pixel Information Recipients because Defendant kept this information secret.

CLASS ALLEGATIONS

180. This action is brought by the named Plaintiffs on their behalf and on behalf of a proposed Class of all other persons similarly situated under Rule 23 of the Nevada Rules of Civil Procedure.

181. 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 Pixels and other tracking technologies on Defendant's Website.

182. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff W.M.F. asserts claims on behalf of a separate Nevada Subclass, which is defined as follows:

> All persons residing in the State of Nevada whose Private Information was disclosed to a third party without authorization or consent through the Pixels and other tracking technologies on Defendant's Website.

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

184. Plaintiffs reserve the right to amend the definitions of the Class and the Subclass or add subclasses if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

185. **Numerosity**. The Class is so numerous that the individual joinder of all members is impracticable. There are at least 390 thousand patients that have been impacted by Defendant's actions. Moreover, the exact number of those impacted is generally ascertainable by appropriate discovery and is in the exclusive control of Defendant.

186. **Commonality.** Common questions of law or fact arising from Defendant's conduct exist as to all members of the Class, which predominate over any questions affecting only individual Class Members. These common questions include, but are not limited to, the following:

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

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

c) Whether Defendant violated its own privacy policy by disclosing the Private Information of Plaintiffs and Class Members to the Pixel Information Recipients;

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

e) Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class

Members that their Private Information was being disclosed without their consent;

f) Whether Defendant adequately addressed and fixed the practices which permitted the unauthorized disclosure of patients' Private Information;

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

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

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

j) Whether Defendant knowingly made false representations as to their data security and/or privacy policy practices;

k) Whether Defendant knowingly omitted material representations with respect to their data security and/or privacy policy practices and

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

187. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised as a result of Defendant's incorporation and use of the Pixels and/or Conversions API.

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

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

190. Superiority. A class action is superior to other available methods for the fair and

efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

191. Defendant has acted on grounds that apply generally to the Class as a whole so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis under NRCP 23(c)(2).

192. 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 Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information and not disclosing it to unauthorized third parties;

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

c) Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

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

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

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

193. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the unauthorized disclosures that have taken place. Class Members have already been preliminarily identified and sent Notice by Defendant.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(*On behalf of Plaintiffs & the Nationwide Class*)

194. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

195. Upon soliciting, accepting, storing, and controlling the Private Information of Plaintiffs and the Class, Defendant owed, and continue to owe, a duty to Plaintiffs and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information.

196. Defendant breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

197. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information through their use of the Pixels, Conversions API, and other tracking technologies would result in unauthorized third parties, such as the Pixel Information Recipients, gaining access to such Private Information for no lawful purpose.

198. Defendant's duty of care to use reasonable measures to secure and safeguard Plaintiffs' and Class Members' Private Information arose due to the special relationship that existed between Defendant and their patients, which is recognized by statute, regulations, and the common law.

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

200. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their Private Information. Defendant's misconduct included the failure to (1) secure Plaintiffs' and Class Members' Private Information; (2) comply with industry standard data security

practices; (3) implement adequate website and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Pixels, Conversions API, and other tracking technologies.

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

202. Defendant's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiffs' and Class Members' Private Information constituted (and continue to constitute) negligence at common law.

203. Plaintiffs and the Class are entitled to recover damages in an amount to be determined at trial.

COUNT II
INVASION OF PRIVACY
(*On behalf of Plaintiffs & the Nationwide Class*)

204. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

205. The highly sensitive and personal Private Information of Plaintiffs and Class Members consists of private and confidential facts and information regarding Plaintiffs' and Class Members' health that were never intended to be shared beyond private communications on the Website and the consideration of health professionals.

206. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this Information against disclosure to unauthorized third parties, including the Pixel Information Recipients.

207. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

208. Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Private

Information to the Pixel Information Recipients—third-party tech and marketing giants who use such information for their own business purposes—is highly offensive to a reasonable person.

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

210. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiffs' and Class Members' privacy because Defendant facilitated the Pixel Information Recipients' simultaneous eavesdropping and wiretapping of confidential communications.

211. Defendant failed to protect Plaintiffs' and Class Members' Private Information and acted knowingly when they installed the Pixels onto the Website because the purpose of the Pixels is to track and disseminate individual's communications on the Website for the purpose of marketing and advertising.

212. Because Defendant intentionally and willfully incorporated the Pixels into the Website and encouraged individuals to use and interact with the Website and the health services thereon, Defendant had notice and knew that their practices would cause injury to Plaintiffs and the Class.

213. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information, such as the IIHI and PHI of Plaintiffs and Class Members, was disclosed to unauthorized third parties, causing Plaintiffs and the Class to suffer damages.

214. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, lost benefit of the bargain, plus pre-judgment interest and costs.

215. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information is still maintained by Defendant and still in the possession of the Pixel Information Recipients, and the wrongful disclosure of the Private Information cannot be undone.

216. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's and unauthorized third parties' continued possession of their sensitive and confidential Private Information. A judgment for monetary damages will not undo Defendant's disclosure of the Private Information to unauthorized third parties who continue to possess and utilize the Private Information.

217. Plaintiffs, on behalf of themselves and Class Members, further seek injunctive relief to enjoin Defendant from intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT III
BREACH OF CONFIDENCE
(*On behalf of Plaintiffs & the Nationwide Class*)

218. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

219. Possessors of non-public medical information, such as Defendant, have a duty to keep such medical information completely confidential.

220. Plaintiffs and Class Members had reasonable expectations of privacy in the responses and communications entrusted to Defendant through their Website, which included highly sensitive Private Information.

221. Contrary to its duties as a telehealth services provider and its express promises of confidentiality, Defendant installed the Pixels and Conversions API to disclose and transmit to third parties Plaintiffs' and Class Members' Private Information, including data relating to Plaintiffs' and Class Members' health.

222. These disclosures were made without Plaintiffs' or Class Members' knowledge, consent, or authorization.

223. The third-party recipients included, but may not be limited to, the Pixel Information Recipients.

224. As a direct and proximate cause of Defendant's unauthorized disclosures of Plaintiffs' and Class Members' Private Information, Plaintiffs and Class Members were damaged by Defendant's

breach of confidentiality in that (a) sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private; (b) Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements; (c) Defendant eroded the essential confidential nature of health services that Plaintiffs and Class Members participated in; (d) general damages for invasion of their rights in an amount to be determined by a jury at trial; € nominal damages for each independent violation; (f) the unauthorized use of something of value (the highly sensitive Private Information) that belonged to Plaintiffs and Class Members and the obtaining of a benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation to Plaintiffs or Class Members for the unauthorized use of such data; (g) diminishment of the value of Plaintiffs' and Class Members' Private Information and (h) violation of property rights Plaintiffs and Class Members have in their Private Information.

COUNT IV
UNJUST ENRICHMENT
(*On behalf of Plaintiffs & the Nationwide Class*)

225. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

226. Defendant has benefitted from the use of Plaintiffs' and Class Members' Private Information and unjustly retained those benefits at Plaintiffs' and Class Members' expense.

227. Plaintiffs and Class Members conferred a benefit upon Defendant in the form of the monetizable Private Information that Defendant collected from them and disclosed to third parties, including the Pixel Information Recipients, without authorization and proper compensation.

228. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

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

230. The benefits that Defendant derived from Plaintiffs and Class Members were not

offered by Plaintiffs or Class Members gratuitously and, thus, rightly belongs to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles in any state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

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

COUNT V
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(1), *et seq.*
(*On behalf of Plaintiffs & the Nationwide Class*)

232. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein.

233. The ECPA protects both sent and received communications.

234. The ECPA, specifically 18 U.S.C. § 2520(a), provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

235. The transmissions of Plaintiffs' and Class Members' Private Information to Defendant via Defendant's Website is a "communication" under the ECPA's definition under 18 U.S.C. § 2510(12).

236. The transmission of Private Information between Plaintiffs and Class Members and Defendant via their Website are "transfer[s] of signs, signals, writing, … data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

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

238. The ECPA defines "interception" as the "acquisition of the contents of any wire,

electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

239. The ECPA defines "electronic, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5).

240. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's webservers and

d. The Pixels deployed by Defendant to effectuate the sending and acquisition of user and patient sensitive communications.

241. By utilizing and embedding the Pixels and Conversions API on their Website and/or servers, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

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

243. Defendant's intercepted communications that included, but are not limited to, communications to/from Plaintiffs and Class Members regarding their IIHI and PHI, including IP address, Facebook ID, and health information relevant to the screenings and treatment plans in which Plaintiffs and Class Members participated.

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

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

246. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

247. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixels and Conversions API to track and utilize Plaintiffs' and Class Members' Private Information for its own financial benefit.

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

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

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

251. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendant's Website, creation of accounts, participation in Defendant's health screenings, and/or purchasing a subscription plan, Defendant's purpose was tortious and designed to violate federal and state law, including as described above, a knowing intrusion into a private place, conversation, or matter that would be highly offensive to a reasonable person.

COUNT VI
VIOLATIONS OF THE NEVADA CONSUMER FRAUD ACT
NRS Ch. 41.600
(*On behalf of Plaintiff W.M.F. & the Nevada Subclass*)

252. Plaintiff W.M.F. re-alleges and incorporates by reference the allegations above as if fully set forth herein.

253. Plaintiff W.M.F. has a private right action pursuant to NRS 41.600(2)(e).

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

255. Plaintiff and Class members relied on Defendant's implied promise of data privacy and security when providing their Private Information to Defendant.

256. The Nevada Deceptive Trade Practices Act ("NDTPA"), codified in NRS Chapter 598, prohibits unfair and deceptive trade practices in the course of any business or occupation.

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

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

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

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

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

advertised," *i.e.*:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff W.M.F.'s and Nevada Subclass Members' Private Information from unauthorized disclosure;

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

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff W.M.F.'s and Nevada Subclass Members' Private Information from unauthorized disclosure;

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

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

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

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

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

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

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

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

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

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

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

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Classes, respectfully request that this Court enter an Order:

a) Certifying this case as a class action on behalf of the Nationwide Class and the Nevada Subclass defined above, appointing Plaintiffs as representatives of the Class, and appointing their counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or unauthorized disclosure of Plaintiffs' and Class Members' Private Information;

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

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

e) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

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

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

Dated: November 25, 2024

Respectfully submitted,

/s/ Michael Kind

MICHAEL KIND, ESQ.
Nevada Bar No.: 13903
KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, Nevada 89123
Telephone: (702) 337-2322
Facsimile: (702) 329-5881
Email: mk@kindlaw.com

ALMEIDA LAW GROUP LLC
David S. Almeida (*pro hac vice* anticipated)
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024
david@almeidalawgroup.com

MIGLIACCIO & RATHOD LLP
Nicholas Migliaccio (*pro hac vice* anticipated)
Jason Rathod (*pro hac vice* anticipated)
Bryan G. Faubus (*pro hac vice* anticipated)
412 H St. NE

Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730
nmigliaccio@classlawdc.com
jrathod@classlawdc.com
bfaubus@classlawdc.com

Attorneys for Plaintiffs & Proposed Classes