UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

KAYE LOCKREM and TERRI CASSICK, Plaintiffs, v. GROUP HEALTH PLAN, INC. d/b/a/ HEALTHPARTNERS Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Kaye Lockrem and Terri Cassick (collectively, "Plaintiffs"), on behalf of themselves and on behalf of all others similarly situated ("Class Members"), bring this Consolidated Amended Class Complaint against Group Health Plan, Inc. d/b/a HealthPartners ("HealthPartners" or "Defendant") and allege, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this case to address Defendant's transmission and disclosure of Plaintiffs' and Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information" or "PII and PHI") to Meta Platforms, Inc. d/b/a Meta ("Facebook"), among other third parties, via a tracking pixel ("Tracking Pixel" or "Pixel") installed on Defendant's websites www.healthpartners.com and www.virtuwell.com (collectively referred to as "Website"), which it owns and controls.

2. Defendant is the largest consumer governed nonprofit health care organization in the nation, serving more than 1.8 million medical and dental health plan members across several states. HealthPartners is a covered entity under the Health Insurance Protability and Accountability Act of 1996, 42 U.S.C. § 1320 d, 45 C.F.R. Part 160-45 Part 162, and 45 C.F.R. Part 164 (hereinafter "HIPAA').

3. Plaintiffs' and Class Members' Private Information that was unlawfully intercepted and transmitted to Facebook and other third parties by Defendant includes the following: IP addresses; dates, times, and/or locations of scheduled appointments; medical symptoms and conditions, proximity to a Defendant related healthcare location; information about provider; types of appointments or procedures; communications between patients and others through the Website, which may have included first and last names and medical record numbers; insurance information; and medical related private information.

4. In order to provide medical treatment and care, Defendant collects and stores patients' Private Information, including their medical records. In doing so, Defendant has statutory, regulatory, contractual, fiduciary, and common law duties to safeguard that Private Information from disclosure and ensure that it remains private and confidential. Defendant is duty bound to maintain the confidentiality of patient medical records and information and is further required to do so by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[1]

5. Plaintiffs and Class Members are individuals who have sought and may continue to seek medical services, advice, consultation, and/or treatment from Defendant, or its related healthcare entities. Defendant advertises its online services on its Website, to assist patients with

[1] The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996), ("HIPAA"), and regulations of the United States Department of Health and Services ("HHS") promulgated thereunder, are designed to protect the confidentiality and guard against the unauthorized disclosure of medical records, patient health care information, and other individually identifiable healthcare information.

their medical care. Based on Defendant's encouragement that patients use its online services, Plaintiffs used the Defendant's Website to search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from their healthcare providers, receive lab results, review medical records, and exchange insurance information.

6. Plaintiffs are further informed and believe that since information transmitted via the Pixel was linked to their personal Facebook account, Defendant also installed and implemented Facebook's Conversion Application Programming Interface (Conversion API) on its Website, thereby surreptitiously enabling further or additional transmissions and disclosures of Plaintiffs' and Class Members' Private Information, which is stored as well by virtue of Plaintiffs' visiting Defendant's Website.

7. Facebook, in turn, accessed, intercepted, received, collected, stored, and used and exploited for pecuniary gain, Plaintiffs' and Class Members' Private Information to target advertisements to Plaintiffs and Class Members based on the Private Information disclosed by Plaintiffs and Class Members to Defendant.

8. Accordingly, the purpose of this lawsuit is to protect Plaintiffs' and Class Members' right to protect their Private Information and seek remedies for the harm caused by Defendant's intentional, reckless, or negligent disclosure to third parties, such as Facebook, as a consequence of Defendant's installation on its Website of the Facebook Tracking Pixel, which secretly enables, the interception, transmission and disclosure of Plaintiffs HIPAA protected Private Information, (which includes PII and PHI), as they are communicated to Defendant in real time, and Defendant's installation and implementation of the Companion Facebook Application Programming Interface (Conversion API) on its Website.

BACKGROUND

9. When an individual visits the Defendant's Website and submits Private Information to Defendant, its Tracking Pixel transmits that Private Information to third parties, such as Facebook and others. A pixel is a piece of code that "tracks the people and [the] type of actions they take."[2] Pixels are used to target specific customers by utilizing the data gathered through the Defendant's Website to build profiles for the purposes of retargeting[3] and future marketing.

10. For instance, with respect to Facebook, the persistent Facebook Pixel on Defendant's Website causes that individual's unique and persistent Facebook ID ("FID") to be transmitted alongside other Private Information that is sent to Facebook.

11. Upon information and belief, Defendant utilized the Pixel data to improve and save costs on its marketing campaign, improve its data analytics, attract new patients, and market new services and/or treatments to its existing patients. In other words, Defendant implemented the Tracking Pixel to bolster its profits.

12. Pixels are routinely used to target advertising to specific customers by utilizing the data gathered through the pixel to build profiles for the purposes of retargeting and future marketing.

13. In this context, the Pixel is designed to report to third parties data gathered about the web page currently visited and any information to/from the User to the web page. In other words, a pixel creates a link – hidden from the website's user – that transfers information sent to/from the web page to the third party.

---

[2] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Feb. 22, 2023).

[3] "Retargeting" or "remarketing" is a form of advertising that displays ads or sends emails to previous visitors of a particular website who did not "covert" the visit into a sale or otherwise meet a marketing goal of the website owner.

14. Operating as designed, Defendant's Pixel allowed the Private Information that Plaintiffs and Class Members submitted to Defendant to be unlawfully disclosed to third parties, including Facebook.

15. For example, when Plaintiffs or a Class Member accessed Defendant's Website hosting the Pixel, the Pixel software directed Plaintiffs' or Class Members' browser to send a message to the third party's servers. The information sent to third parties by Defendant included the Private Information that Plaintiffs and Class Members submitted to Defendant's Website, including, for example, the type and date of a medical appointment and physician. Such Private Information would allow the third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care and the type of medical care being sought. This disclosure would also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, or HIV.

16. The third party, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who online target[4] Plaintiffs and Class Members based on communications obtained via the Tracking Pixel.

17. Plaintiffs submitted medical information to Defendant's Website, including the Website used to search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from their healthcare providers, receive lab results, review medical records, and exchange insurance information.

18. Defendant regularly encouraged Plaintiffs and Class Members to use its digital tools, including its Website, to receive healthcare services. In doing so, Defendant also directed

[4] "Online Targeting" is "a process that refers to creating advertisement elements that specifically reach out to prospects and customers interested in offerings. A target audience has certain traits, demographics, and other characteristics, based on products or services the advertiser is promoting." *See* https://digitalmarketinggroup.com/a-guide-to-online-targeting-which-works-for-your-business/ (last visited: Feb. 22, 2023).

Plaintiffs and Class Members to its Privacy Policies, which preclude the transmission or disclosure of Private Information to unauthorized third parties, such as Facebook.

19. Conversations API enables business entities to send web communications from their servers to Facebook. Conversion API, by design, establishes a direct, reliable connection between marketing data communicated on websites, for example, between Defendant's server to Facebook, consequently storing Plaintiffs and Class Members' Private Information on Defendant's server, which is then transmitted to Facebook. Hence, Conversions API provides yet an additional method of tracking beyond the Pixel. Importantly, there are no privacy protections on the users' end that can bypass or defeat the Conversations API.

20. Conversations API effectively tracks Plaintiffs' and Class Members' website interaction, including their Private Information, which is transmitted to Facebook. Facebook actually boasts in its efforts to market Conversion API that it provides a "better measure [of] add performance and attribution across your customer's full journey, from discovery to conversion" and that this "helps you better understand how digital advertising impacts both online and offline results."

21. Plaintiffs and Class Members provided Private Information to Defendant in order to receive medical services and with the reasonable expectation that Defendant would protect their Private Information.

22. Defendant made express and implied promises to protect Plaintiffs' and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchange with Defendant.

23. At all times that Plaintiffs and Class Members visited and utilized Defendant's Website, they had a reasonable expectation of privacy in the Private Information collected through

Defendant's Website, including that it would remain secure and protected and only utilized for medical purposes. Plaintiffs' and Class Members' expectations were entirely reasonable because (1) they are patients; and (2) Defendant is a healthcare provider which is required by common and statutory law to protect its patients' Private Information. Moreover, Plaintiffs and Class Members also relied on the Defendant's Privacy Policies, which do not permit the transmission or disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties.

24. 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 those individuals to protect and safeguard that information from unauthorized disclosure.

25. However, as set forth more fully below, Defendant failed in its obligations and promises by utilizing the Pixel on its Website and/or deploying and installing Conversions API, knowing that such technology would transmit and disclose Plaintiffs' and Class Members' Private Information to unauthorized third parties, including Facebook, for example.

26. Defendant did not disclose to Plaintiffs or Class Members that it shared their sensitive and confidential communications to Facebook or other third parties. As a result, Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously transmitted and/or disclosed to Facebook and/or other third parties as they communicated with their healthcare provider via the Website.

27. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web based technology to ensure the Defendant's Website was safe and secure; (ii) failing to remove or disengage technology that was known and

designed to share web-users' information; (iii) failing to obtain the consent of Plaintiffs and Class Members to disclose their PII and PHI to Facebook, or other third parties; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' PII and PHI through the Pixel or Conversions API; (v) failing to warn Plaintiffs and Class Members; and (vi) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient PII and PHI.

28. Plaintiffs and Class Members have suffered injury as a result 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 Pixel and/or Conversions API, (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information, (v) statutory damages, and (vi) the continued and ongoing risk of exposure of their Private Information.

29. Plaintiffs seek to remedy these harms and bring causes of action for (1) Invasion of Privacy; (2) unjust enrichment; (3) breach of implied contract; (4) breach of confidence; (5) violations of the Electronics Communication Privacy Act ("ECPA") 18 U.S.C. § 2511(1) - unauthorized interception, use, and disclosure; (6) violations of ECPA, 18 U.S.C. § 2511(3)(a) - unauthorized interception, use, and disclosure; (7) violations of Title II of the ECPA, 18 U.S.C. § 2702, *et seq.*, - Stored Communications Act; (8) violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*; and (9) violations of the Minnesota Uniform Deceptive Trade Practices Act ("MUDTPA") Minn. Stat. § D. 43-48.

PARTIES

Plaintiff Kaye Lockrem

30. Plaintiff Lockrem is a national person and citizen of Maplewood, Minnesota. Plaintiff Lockrem has been a healthcare patient with respect to a HealthPartners healthcare facility, and has accessed Defendant's Website on various occasions.

31. Plaintiff Lockrem's Private Information was disclosed to Facebook, which information included PII, PHI, and related confidential information that Defendant intercepted and/or assisted being intercepted by Facebook and other third parties, without Plaintiff's consent, written authorization or knowledge, and thereby breaching Plaintiff's confidentiality by doing so.

32. Plaintiff Lockrem has been a Facebook user starting in the Fall of 2006.

33. Plaintiff Lockrem accessed Defendant's Website in order to receive healthcare services from Defendant or its affiliates, and did so in accordance with Defendant's directions and encouragement.

34. Plaintiff Lockrem reasonably expected, at all time material, that these communications with Defendant, irrespective of whatever medium was used, and in particular, any such communications with Defendant online, would remain confidential, and would not be transmitted, intercepted, accessed, used or otherwise exploited by Facebook, or any other third party, nor would Defendant permit such Private Information, including PII and PHI, to be intercepted by any third party, such as or including Facebook.

Plaintiff Terri Cassick

35. Plaintiff Cassick is a natural person and citizen of Torrance, California.

36. Plaintiff Cassick has been a health care patient with respect to HealthPartners health care facility, and has accessed Defendant's Website on various occasions.

37. Plaintiff Cassick's Private Information was disclosed to Facebook, which information included PII, PHI, and related confidential information that Defendant intercepted and/or assisted being intercepted by Facebook and other third parties, without Plaintiff's consent, written authorization or knowledge, and thereby breaching Plaintiff's confidentiality by doing so.

38. Plaintiff Cassick has been a Facebook user starting in 2009.

39. Plaintiff Cassick accessed Defendant's Website in order to receive health care services from Defendant or its affiliates, and did so in accordance with Defendant's directions and encouragement.

40. Plaintiff Cassick reasonably expected, at all times material, that these communications with Defendant, irrespective of whatever medium was used, and in particular, any such communications with Defendant online, would remain confidential, and would not be transmitted, intercepted, accessed, used, or otherwise exploited by Facebook, or any other third party, nor would Defendant permit such Private Information, including PII and PHI, to be intercepted by any third parties such as or including Facebook.

41. At all times material, Plaintiffs relied on Defendant's Privacy Policies which further provided a reasonable expectation that Defendant would maintain and safeguard the confidentiality of her information, including their Private Information, which they would never have disclosed in any event to Defendant had they not been a patient or recipient of healthcare services from Defendant or Defendant's affiliates.

42. Plaintiffs have never consented to the transmission of their Private Information by Defendant directly or indirectly, to Facebook, or third parties, or their usage, and have never consented to their access or interception of such information by them.

43. Plaintiffs are informed and believe and thereupon allege that irrespective of their lack of consent or permission, and as a consequence of the Facebook Pixel and Conversions API, Defendant enabled or otherwise transmitted their Private Information, including their PII or PHI to Facebook, and other third parties, in violation of their privacy rights and federal and state law and statute, as discussed below much to their substantial detriment and harm.

Defendant HealthPartners

44. Defendant Group Health, Inc., d/b/a HealthPartners, maintains its principal place of business and headquarters at 8170 33rd Avenue, South Bloomington, Minnesota. Founded in 1957 as a cooperative, Defendant has grown to be the largest consumer govern non-profit health care organization in the Nation, serving over 1.8 medical and dental health care members nationwide. Defendant provides healthcare services and health plan financing and administration, and its system includes multi-specialty group practices of more than 1,800 physicians serving more than 1.2 million patients, employing over 26,000 people.[5]

45. Defendant was and has been at all time material a covered entity under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 132.0(d) and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164, (hereinafter referred to as HIPAA).

JURISDICTION

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

[5] https://www.healthpartners.com/about/ (last visited February 21, 2023).

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

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

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

COMMON FACTUAL ALLEGATIONS

Defendant Improperly Disclosed Plaintiffs' and Class Members' Private Information via the Pixel and Conversions API.

50. Defendant utilizes its Website to connect Plaintiffs and Class Members to Defendant's healthcare platform with the goal of increasing profitability.

51. To accomplish this, Defendant utilized the Pixel and Facebook's Conversion API in connection with offering its healthcare related services to Plaintiffs and Class Members. While seeking and using Defendant's services as a medical provider, and utilizing the Website, Plaintiffs' and Class Members' Private Information was intercepted in real time and then disseminated to Facebook, and other third parties, via the Pixel and to Facebook via the Conversions API that Defendant installed on its Website.

52. Plaintiffs and Class Members did not intend or have any reason to suspect the Private Information would be shared with Facebook, or other third parties, or that Defendant was tracking their every communication and disclosing the same to third parties when they entered Private Information on Defendant's Website.

53. Defendant did not disclose to or warn Plaintiffs or Class Members that Defendant used Plaintiffs' and Class Members' confidential electronic medical communications and Private Information for marketing purposes.

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

55. Upon information and belief, Defendant intercepted and disclosed the following non-public Private Information to Facebook and other third parties:

a. Plaintiffs' and Class Members' status as medical patients;

b. Plaintiffs' and Class Members' communications with Defendant through its Website;

c. Plaintiffs' and Class Members' medical appointments, location of treatments, specific medical providers, and specific medical conditions and treatments;

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

Defendant's Transmission of Private Information via the Pixel and Conversions API: The Pixel, Source Code and HTTP Requests Interaction

57. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as computer, tablet, or smart phone) accessed web content through a web browser.

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

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

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

60. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as a physician's "Book an Appointment" page), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Webpage(s)).

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

62. Source code may additionally 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. The Pixel – source code – does just that, acting much like a traditional wiretap. When patients visit Defendant's website via an HTTP Request to Aurora's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel. In essence, Defendant is handing patients a tapped phone, and once the Webpage is loaded into the patient's browser, the software-based wiretap is silently waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook.

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

64. Facebook, implements workarounds that cannot be evaded by savvy internet users. Here, its workaround is called Conversions API, which is effective because it does not intercept data communicated from the user's browser. Instead, Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]." Communications between patients and Defendant using 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.

65. Companies like Facebook instruct Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[6] Upon information and belief, Facebook's customers who implement the Facebook Pixel in accordance with Facebook's documentation also implement the Conversions API workaround.

66. Without any knowledge, authorization, or action by users such as Plaintiffs, a website owner like Defendant can use its Source Code to commandeer each user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

67. In this case, Defendant employed just such a device to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to Facebook.

68. As an example, upon information and belief, when Plaintiffs visited www.healthpartners.com/care/speciality/ and selected a specific subject matter, their browser automatically sends an HTTP Request to Defendant's web server which, automatically, returns an HTTP Response, and loads the Markup for that particular webpage. Any patient visiting such a

[6] *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Feb. 22, 2023).

webpage with respect to that particular topic, would only see the "Markup," but not the Defendant's Source Code or underlying HTTP Request and responses.

69. Meanwhile, the Source Code can execute other programmatic instructions such as, for example, commanding of website visitors browser to send data transmissions to third parties via Pixels or web bugs, which in effect, creates a spying window through which the webpage can funnel the visitors data, actions and communications to third parties, including, for example, Facebook.

70. Defendant's Source Code is able to manipulate the patient's browser by secretly instructing it to duplicate their communications (HTTP Request) and send such communications to Facebook. This is enabled by the Pixel embedded in Defendant's Source Code, which has been programmed to automatically track and transmit such communications, which tracking and transmission occurs contemporaneously, and visibly, and without the Plaintiff's or patient's knowledge or consent.

71. In effect, Defendant uses its Source Code to take over patient's computing devices, and redirect their Private Information to third parties such as Facebook.

72. As soon as Plaintiffs and Class Members visited Defendant's Website and communicated their Private Information, it was transmitted to Facebook, which information included various aspects that were covered and considered confidential under HIPAA, and which were not permitted to be intercepted, transmitted, or otherwise provided to or accessed by any third parties.

Facebook's Platform and its Business Tools

73. Facebook operates the world's largest social media company.

74. In 2021, Facebook generated $117 billion in revenue.[7] Roughly 97% of that came from selling advertising space.[8]

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

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

77. Facebook then sells advertising space by highlighting its ability to target users.[9] Facebook can target users so effectively because it surveils user activity both on and off its site.[10] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[11] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[12]

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

79. Advertisers can also build "Custom Audiences."[13] Custom Audiences enable advertisers to reach "people who have already shown interest in [their] business, whether they're

---

[7] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Feb. 22, 2023)
[8] *Id.*
[9] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706 (last visited Feb. 22, 2023).
[10] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Feb. 22, 2023).
[11] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Feb. 22, 2023).
[12] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences (last visited Feb. 22, 2023).
[13] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited Feb. 22, 2023).

loyal customers or people who have used [their] app or visited [their] website."[14] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[15] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools," including the Facebook Pixel.[16]

80. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[17] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept, collect, view, and use user activity on those platforms.

81. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[18] Facebook's Business Tools

---

[14] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Feb. 22, 2023).
[15] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited Feb. 22, 2023).
[16] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited Feb. 22, 2023).
[17] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087 (last visited Feb. 22, 2023).
[18] *See* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Feb.

can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[19] Advertisers can even create their own tracking parameters by building a "custom event." [20]

82. One such Business Tool is the aforesaid Facebook Pixel. Facebook offers this piece of code to advertisers, like Defendant, to integrate into their websites. As the name implies, the Facebook Pixel "tracks the people and type of actions they take."[21] When a user accesses a website hosting the Facebook Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers at certain times during interaction with the webpage. This second, secret transmission contains the original 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 Websites—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 and treatment requests but also their home address, zip code, or phone number. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[22] The Plaintiffs' and Class Members' identities can be easily

---

22, 2023).

[19] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (Last visited Feb. 22, 2023)

[20] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/. (Last visited Feb. 22, 2023)

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

[22] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (Last visited Feb. 22, 2023)

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

84. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the Website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity.

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

The Pixel and/or Conversions API Effectively Caused Private Information of Plaintiffs, Which Was Protected by HIPAA, to be Intercepted, Transmitted, Shared, and Stored and Also Exploited by Facebook

86. Plaintiffs are informed and believe and thereupon allege that Defendant installed the Facebook Pixel and Conversions API on its website which, as a consequence, enabled it to secretly track patients, recording their activity and experiences as they utilize the website for medical health purposes.

87. The Pixel helped Defendant to effectively better target the delivery of advertising and measure consumer audiences for marketing purposes, while decreasing its own advertising and marketing cost. Defendant's webpages contained a unique identifier demonstrating that the Pixel was being used on a particular webpage identified as 1113456592041476 on

www.healthpartners.com and 200310607002735 on www.virtual.com. Plaintiffs and Class Members were unaware that when they communicated their Private Information to Defendant via its Website, such information was being shared with Facebook as it was communicated to Defendant, in real time.

88. Defendant did not disclose this particular and important, material information to Plaintiffs and Class Members, nor did they consent, agree to, authorize, or otherwise knowingly permit Defendant to disclose their Private Information to Facebook or otherwise exploit it for pecuniary gain, and did not intend that Facebook even be a party to their communications of Private Information with Defendant, to whom they were directing such communications for the purposes of healthcare.

89. Contemporaneous with Plaintiffs provision of their Private Information to Defendant which, via its Pixel, and/or Conversions API, was then transmitted to Facebook, were their Facebook ID (c_usercookie or "FID"), which thereby enabled individual patient's communications with Defendant, and the Private Information contained therein, to be linked to their unique Facebook accounts.[23]

90. Defendant's implementation of the Facebook Pixel and Conversions API, surreptitiously tracking, recording and disclosing Plaintiffs' and other Class Members'/patient confidential communications and Private Information, and disclosing such protected information to Facebook – an authorized third party – while secretly undertaking this pattern of conduct without Plaintiffs' or Class Members' expressed written consent or permission, violated their privacy rights.

[23] The FID is linked to a user's Facebook profile. It typically contains demographic and other information about the user. Since the user's Facebook Profile FID uniquely identifies an individual's Facebook account, Meta-or any ordinary person – can easily use the Facebook profile ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

Defendants Privacy Policies and Promises

91. Plaintiffs and Class Members using Defendant's Website were informed that its privacy policies were styled and followed in order to maintain the privacy and confidentiality of their Private Information, and that any disclosure of such information would be under certain limited circumstances (which do not apply here).[24]

92. Defendant's Notice of Privacy Practices explains its legal duties regarding Private Information, while outlining those instances when Defendant could or would lawfully use and disclose Plaintiffs' and Class Members' Private Information to third parties, noting the following instances of exception:

- Follow the law;
- Help with public health and safety issues;
- Respond to organ and tissue donation requests;
- Work with a medical examiner or funeral director;
- Handle workers' compensation;
- Respond to lawsuits and legal actions; and
- With your written permission

93. The Privacy Policy or Practices represented by the Defendant never permitted it to intercept, transmit, disclose, or otherwise exploit Plaintiffs' and Class Members' Private Information to third parties, including Facebook, and, in particular, do not permit it to do so for marketing purposes, whether for Defendant or for Facebook, or any other third party.

[24] https://www.healthpartners.com/ucm/groups/public/@hp/@public/documents/documents/cntrb_009405.pdf (last visited Feb. 22, 2023).

94. Defendant acknowledges in its Privacy Policy that it is required to maintain the confidentiality of Plaintiffs' and Class Members' Private Information, absent one of the foregoing exceptions, and that this is a requirement by law.

95. However, and despite its privacy policies, HIPAA standards, and industry standards, Defendant knowingly violated its own Privacy Policy and law by intercepting and disclosing Plaintiffs' and Class Members' Private Information to Facebook and third parties, absent fully informing and disclosing them that it shares their Private Information with such third parties, and without securing their specific consent or authorization, to so share their Private Information.

Defendant Violated HIPAA Standards

96. 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.[25]

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

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

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[26]

[25] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[26] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022)

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

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added).[27]

100. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[28]

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

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

Defendant Violated Industry Standards

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

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

105. AMA Code of Ethics Opinion 3.1.1 provides:

[27] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Nov. 3, 2022)
[28] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

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

106. 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.

107. 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.

Plaintiffs' and Class Members' Expectation of Privacy

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

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

IP Addresses are Personally Identifiable Information

110. On information and belief, through the use of the Tracking Pixels on the Defendant's Website, Defendant also disclosed and otherwise assisted Facebook, Google, and/or other third parties with intercepting Plaintiffs' and Class Members' Computer IP addresses.

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

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

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

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

115. Google also tracks IP addresses associated with Internet users.

116. Facebook, Google, and other third-party marketing companies track IP addresses for use in tracking and targeting individual homes and their occupants with advertising by using IP addresses.

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

a. HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

b. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

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

Defendant was Enriched and Benefitted from its Surreptitious Conduct Due to the Pixel and Conversion API Unauthorized Disclosures

119. The sole purpose of the use of the Tracking Pixel on Defendant's Website was marketing and profits, as was the purpose of the conversion API that was also installed and that also benefitted Facebook.

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

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

122. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients, including Plaintiffs and Class Members.

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

TOLLING

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

CLASS ACTION ALLEGATIONS

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

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

> **All individuals residing in the United States whose Private Information was disclosed to Facebook or third parties without authorization or consent**

through the Tracking Pixel or Conversion API on Defendant's Website, (the "Nationwide Class").

127. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff Lockrem asserts claims on behalf of a separate subclass, defined as follows:

All individuals residing in Minnesota whose Private Information was disclosed to Facebook or third parties without authorization or consent through the Tracking Pixel or Conversion API on Defendant's Website (the "Minnesota Class").

128. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiff Cassick assert claims on behalf of a separate subclass, defined as follows:

All individuals residing in California whose Private Information was disclosed to Facebook or third parties without authorization or consent through the Tracking Pixel or Conversion API on Defendant's Website (the "California Class").

129. Excluded from the Nationwide Class, Minnesota Class, and California Class (sometimes collectively referred to as "Class") are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

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

131. Numerosity, Fed R. Civ. P. 23(a)(1). The Class Members for each proposed Class are so numerous that joinder of all members is impracticable. Upon information and belief, there are millions of individuals whose Private Information was or may have been improperly transmitted to or accessed by Facebook or third parties, and the Class is identifiable within Defendant's records.

132. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact

common to each Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiffs and Class Members;

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

c. Whether Defendant violated its Privacy Policies by disclosing the PII and PHI of Plaintiffs and Class Members to Facebook, and/or additional third parties.

d. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;

f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient PHI and PII;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;

h. Whether Defendant violated the consumer protection statutes invoked herein;

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 its data security and/or Privacy Policies practices;

k. Whether Defendant knowingly omitted material representations with respect to its data security and/or Privacy Policies 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 PII and PHI.

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

134. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs has 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 has suffered are typical of other Class Members. Plaintiffs has also retained counsel experienced in complex class action litigation, and Plaintiffs intends to prosecute this action vigorously.

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

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

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

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

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

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

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

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

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

b. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information with respect to Defendant's Privacy Policies;

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

d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

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

f. 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

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

143. Plaintiffs reserve the right to amend or modify the Class definition as this case progresses.

COUNT I
INVASION OF PRIVACY
(On Behalf of Plaintiffs, the Nationwide Class, the Minnesota Class, and the California Class)

144. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

145. The Private Information of Plaintiffs and Class Members consists of private and confidential facts and information that were never intended to be shared beyond private communications.

146. 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.

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

148. The unauthorized disclosure to and/or acquisition by a third party social media and marketing giant of Plaintiffs' and Class Members' Private Information via Defendant's Website is highly offensive to a reasonable person.

149. Defendant's willful and intentional disclosure of Plaintiffs' and Class Members'

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

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

151. Defendant failed to protect Plaintiffs' and Class Members' Private Information and acted knowingly when it incorporated the Pixel into its Website because it knew the functionality and purpose of the Pixel.

152. Because Defendant intentionally and willfully incorporated the Pixel into its Website and encouraged patients to use that Website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiffs and Class Members. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiffs and the Class Members was disclosed to a third party without authorization, causing Plaintiffs and the Class to suffer damages.

153. Plaintiffs, on behalf of themselves and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, punitive damages, plus prejudgment interest, and costs.

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

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

156. Plaintiffs, on behalf of themselves and Class Members, further seek injunctive relief to enjoin Defendant from further 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 II
UNJUST ENRICHMENT
(On behalf of Plaintiffs, the Nationwide Class, the Minnesota Class, and the California Class)

157. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

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

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

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

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

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

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

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs, the Nationwide Class, the Minnesota Class, and the California Class)

163. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

164. When Plaintiffs and Class Members provided their user data to Defendant in exchange for services, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

165. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

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

167. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information to third parties, *i.e.*, Facebook.

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

Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members would not have used Defendant's services, or would have paid substantially for these services, had they known their Private Information would be disclosed.

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

COUNT IV
BREACH OF CONFIDENCE
(On behalf of Plaintiffs, the Nationwide Class, the Minnesota Class, and the California Class)

170. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

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

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

173. Plaintiffs' and Class Members' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its Privacy Policies.

174. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Pixel to disclose and transmit Plaintiffs' Private Information and the contents of their communications exchanged with Defendant to third parties.

175. The third-party recipients included, but were not limited to, Facebook.

176. Defendant's disclosures of Plaintiffs' and Class Members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

177. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

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

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

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

c. Defendant took something of value from Plaintiffs and Class members and derived benefit therefrom without Plaintiffs' and Class members' knowledge or informed consent and without compensating Plaintiffs for the data;

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

e. Defendant's actions diminished the value of Plaintiffs' and Class members' Personal Information; and

f. Defendant's actions violated the property rights Plaintiffs and Class members have in their Personal Information.

179. Plaintiffs and Class Members are therefore entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation.

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

180. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

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

182. 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.

183. The transmissions of Plaintiffs' Private Information, which included PII and PHI, to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

184. The transmissions of Plaintiffs Private Information, which included PII and PHI, to the Virtuwell Webpage and medical professionals qualifies as a "communication" under the ELPA's definition in 18 U.S.C. § 2510(2).

185. **Electronic Communications**. The transmission of PII and PHI between Plaintiffs and Class Members and Defendant via its Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

186. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of

that communication." 18 U.S.C. § 2510(8) (emphasis added).

187. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

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

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's web-servers; and

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

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

190. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the Tracking Pixel, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Private Information to third parties such Facebook and Google.

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

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

193. 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).

194. **Unauthorized Purpose**. Defendant intentionally intercepted and caused to be 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.

195. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel and Conversions API to enable the tracking and utilization of Plaintiffs' and Class Members' PII and PHI for financial gain.

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

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

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

199. In sending and in acquiring the content of Plaintiffs' and Class Members'

communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions, including as described above the following: (1) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (2) violation of Minnesota and Illinois statutes as alleged hereinafter.

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

200. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

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

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

203. Defendant's Website is an "electronic communication service" that provides users thereof the ability to send or receive electronic communications. In the absence of Defendant's Website, internet users could not send or receive communications regarding Plaintiffs' and Class Members' PII and PHI.

204. Defendant's Website is a conduit of communication between Plaintiff and Class

Members and their respective medical providers, including third parties who are not employed by Defendant, but contract with Defendant to provide medical treatment and services for its patients.

205. Defendant's Website is also a conduit between Plaintiff and Class Members and the Virtuwell Webpage.

206. **Intentional Divulgence**. Defendant intentionally designed the Tracking Pixel and was or should have been aware that, if misconfigured, it could divulge Plaintiffs' and Class Members' PII and PHI.

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

208. Defendant divulged the contents of Plaintiffs' and Class Members' electronic communications without authorization. Defendant divulged the contents of Plaintiffs' and Class Members' communications to Facebook without Plaintiffs' and Class Members' consent and/or authorization.

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

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"

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

d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

18 U.S.C. § 2511(3)(b)

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

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

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

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

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

214. Moreover, Defendant divulged the contents of Plaintiffs and Class Members'

communications through the Facebook Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

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

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

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

217. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

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

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

220. Defendant intentionally procures and embeds various Plaintiffs' PII and PHI through the Pixel Code used on Defendant's Website, which qualifies as an Electronic Communication Service.

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

222. Defendant stores the content of Plaintiffs' and Class Members' communications on Defendant's Website and files associated with it via the Pixel or Conversions API. As alleged above, Conversions API enables Defendant to store Plaintiffs' and Class Members' Private Information on its servers and then transmit that information to Facebook.

223. When Plaintiffs or Class Member makes a Website communication and/or submission, the content of that communication is immediately placed into storage. As an example, data pertaining to scheduling appointments IP addresses, and communications regarding medical treatment are stored by Defendant.

224. Defendant knowingly divulges the contents of Plaintiffs' and Class Members' communications and from electronic storage through its Website Source Code through workarounds including Facebook's Conversions API.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

229. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications on Defendant's Website to Facebook and third parties were not authorized by 18

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

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

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

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

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

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

COUNT VIII
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (CFAA)
18 U.S.C. § 1030, ET SEQ.
(On Behalf of Plaintiffs and the Nationwide Class)

235. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint

as if fully set forth herein.

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

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

238. Defendant's aforesaid deceptive conduct, i.e. transmitting Private Information to Facebook and third parties under false deceptive means, absent informed consent, caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiffs' and the Class's private and personally identifiable data and content – including the Website visitor's electronic communications with the Website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time ("Website Communications") which were never intended for public consumption.

239. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV) due to the Private Information of Plaintiffs and the Class being made available to Defendant, Facebook, and/or other third parties without adequate legal privacy protections.

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

COUNT IX
Minnesota Uniform Deceptive Trade Practices Act ("MUDPTA") Minn. Stat. §325D.43-48
(On behalf of Plaintiffs, the Nationwide Class, the Minnesota Class, and The California Class)

241. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

242. The MDUPTA prohibits deceptive trade practices in person's business, vocation, or occupation. See Minn. Stat. § 325D.44, subd. 1.

243. Defendant advertised, offered, or sold goods or services in Minnesota and therefore engaged in business directly or indirectly affecting the people of Minnesota, Defendant violated Minn. Stat. § 325D.44, including, but not limited to, the following provisions:

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

b. Engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.

244. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the MDUPTA, including, but not limited to, the following: (1) promising to protect Plaintiffs' and Class Members' Private Information via its Privacy Policies and then, in fact, knowingly, transmitting Plaintiffs' and Class Members' Private Information to third parties, such as Facebook; (2) unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook; (3) failing to disclose or omitting material facts that that Plaintiffs' and Class Members' Private Information would be disclosed to third parties; (4) failing to obtain Plaintiffs' and Class Members' consent in transmitting Plaintiffs' and Class Members' Private Information to Facebook; and (5) knowingly violating industry and legal standards regarding the protection of Plaintiffs' and Class Members' Private Information.

245. These actions also constitute deceptive and unfair acts or practices because Defendant knew its Website contained the Pixel and Conversions API and also knew the Pixel and Conversions API would be unknown and/or not easily discoverable by Plaintiffs and Class Members.

246. Defendant intended that Plaintiff and the Minnesota Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

247. Had Defendant disclosed to Plaintiffs and Class Members that its Website was transmitting PII and PHI to Facebook via the Pixel and Conversions API, said Plaintiffs and Class Members would not have provided their Private Information to Defendant.

248. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Minnesota Class. Plaintiffs and Class Members have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

249. As a result of Defendant's wrongful conduct, Plaintiffs and Class Members were injured in that they never would have provided their PII and PHI to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII and PHI from being taken and misused by others.

250. As a direct and proximate result of Defendant's violations of the MDUPTA, Plaintiffs and Class Members have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiffs and Class Members would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII and PHI; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

251. Pursuant to MDUPTA, Plaintiffs and Class Members are entitled to injunctive relief and other appropriate relief, as alleged.

PRAYER FOR RELIEF

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

A. For an Order certifying the Nationwide Class and each Sub-Class alleged herein, and appointing Plaintiffs and their Counsel to represent each such respective Class;

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

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

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

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

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

Date: February 23, 2023

Respectfully submitted,

/s/ Bryan L. Bleichner
Bryan L. Bleichner (MN Bar No. 0326689)

Jeffrey D. Bores (MN Bar No. 0227699)
Philip J. Krzeski (MN Bar No. 0403291)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
jbores@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Stephen R. Basser* (CA Bar No. 121950)
Samuel M. Ward* (CA Bar No. 216562)
BARRACK RODOS & BACINE
One America Plaza
600 West Broadway, Suite 900
San Diego, California 92101
Phone: (619) 230-0800
Fax: (619) 230-1874
sbasser@barrack.com
sward@barrack.com

John Emerson*
EMERSON FIRM LLP
2500 Wilcrest, Ste. 300
Dallas, Texas 77042
Phone: (800) 551-8649
Fax: (501) 286-4659
jemerson@emersonfirm.com

Counsel for Plaintiffs and Putative Classes

**Bar application forthcoming*