STATE OF WISCONSIN CIRCUIT COURT MILWAUKEE COUNTY

KEEFE JOHN 1812 Pleasant Valley Rd. West Bend, WI 53095 AND JILLIAN CATHERINE KLUG 5758 N. River Forest Dr. Glendale, WI 53209 *on behalf of themselves and all others similarly situated*, Plaintiffs, v. FROEDTERT HEALTH, INC., 9200 W. Wisconsin Ave. Milwaukee, WI 53226 Defendant.	CIV. ACT. FILE NO. _____ **JURY TRIAL DEMANDED**

SUMMONS

THE STATE OF WISCONSIN

To each person named above as a Defendant:

You are hereby notified that the Plaintiffs named above have filed a lawsuit or other legal action against you. The complaint, which is attached, states the nature and basis of the legal action.

Within forty-five (45) days of receiving this summons you must respond with a written answer, as that term is used in Chapter 802 of the Wisconsin Statutes, to the complaint. The court may reject or disregard an answer that does not follow the requirements of the statutes. The answer must be sent or delivered to the court, whose address is 901 N. 9th Street, Room 104, Milwaukee, WI 53233, and to Hansen Reynolds LLC, Plaintiffs' attorneys, whose address is 301 N. Broadway,

Suite 400, Milwaukee, Wisconsin 53202.

You may have an attorney help or represent you. If you do not provide a proper answer within forty-five (45) days, the court may grant judgment against you for the award of money or other legal action requested in the complaint and you may lose your right to object to anything that is or may be incorrect in the complaint. A judgment may be enforced as provided by law. A judgment awarding money may result in a lien against any real estate you own now or in the future, and may also be enforced by garnishment or seizure of property.

Date: March 16, 2023.

Respectfully submitted,

HANSEN REYNOLDS LLC

/s/ Timothy M. Hansen
Timothy M. Hansen (SBN 1044430)
301 N. Broadway, Suite 400
Milwaukee, Wisconsin 53202
(414) 455-7676 (phone)
(414) 273-8476 (fax)
thansen@hansenreynolds.com

ALMEIDA LAW GROUP LLC
David S. Almeida (SBN 1086050)
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024 (phone)
david@almeidalawgroup.com

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
Gary M. Klinger
227 Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

Attorneys for Plaintiffs & the Proposed Class

STATE OF WISCONSIN CIRCUIT COURT MILWAUKEE COUNTY

KEEFE JOHN 1812 Pleasant Valley Rd. West Bend, WI 53095 AND JILLIAN CATHERINE KLUG 5758 N. River Forest Dr. Glendale, WI 53209 *on behalf of themselves and all others similarly situated,* Plaintiffs, v. FROEDTERT HEALTH, INC., 9200 W. Wisconsin Ave. Milwaukee , WI 53226 Defendant.	CIV. ACT. FILE NO. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs KEEFE JOHN AND JILLIAN CATHERINE KLUG (collectively, "Plaintiffs") bring this class action lawsuit in their individual capacities as well as on behalf of all others similarly situated against Froedtert Health, Inc. ("Froedtert" or "Defendant") and allege, upon personal knowledge as to their own actions, their counsel's investigation and upon information and good faith belief as to all other matters, as follows:

1. Plaintiffs bring this class action lawsuit to address Defendant's practice of disclosing Plaintiffs' and Class Members' personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to herein as "Private Information") to third parties, including, but not necessarily limited to, Meta Platforms, Inc. d/b/a Meta

("Facebook").

2. Information about a person's physical and mental health is among the most confidential and sensitive information in our society and the mishandling of medical information can have serious consequences, including, but certainly not limited to, discrimination in the workplace or denial of insurance coverage.[1]

3. Simply put, if people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to much more serious health consequences down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical providers is vitally necessary to maintain public trust in the healthcare system as a whole.

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

[1] *See, e.g.*, Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022), available at https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited March 8, 2023) ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients 'medical history can be inherently criminal and stigmatized."); Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, *"Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies: An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech's tracking tools*, MARKUP (Dec. 13, 2022), available at https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies (last visited March 8, 2023).

5. Defendant owns, controls and maintains a website, https://www.froedtert.com/ (the "Website"), which it encourages patients to use for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, signing up for events and classes, and more.

6. Defendant also maintains a web-based portal called MyChart (the "Portal") and an application (the "App") whereby registered users can make and view appointments, view their health history, review and pay their medical bills, among other things.

7. The Website, the Portal, and the App are collectively referred to herein as the "Web Properties."

8. Plaintiffs and other Class Members who visited and used (collectively, the "Users") Defendant's Web Properties understandably thought they were communicating only with their trusted healthcare providers.

9. Unbeknownst to Plaintiffs and Class Members, however, Defendant had embedded the Facebook Tracking Pixel (the "Pixel" or "Facebook Pixel") on, at least, its Website, which automatically transmits to Facebook every click, keystroke and intimate detail about their medical treatment.

10. Operating as designed and as implemented by Froedtert, the Pixel allows the Private Information that Plaintiffs and Class Members provide to Defendant to be unlawfully disclosed to Facebook alongside the individual's unique and persistent Facebook ID ("FID").[2]

11. A pixel is a piece of code that "tracks the people and [the] type of actions they

[2] The Pixel forces the website user to share the FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser"; "[c]ookies help inform websites about the user, enabling the websites to personalize the user experience." *See* https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited March 8, 2023).

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

12. The user's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner.

13. The Facebook Pixel is thus customizable and programmable, meaning that the website owner (here, Defendant Froedtert) controls which of its web pages contain the Pixel and which events are tracked and transmitted to Facebook.

14. By installing the Facebook Pixel on its Website, Defendant effectively planted a bug on Plaintiffs 'and Class Member's web browsers and compelled them to unknowingly disclose their private, sensitive and confidential health-related communications with Defendant to Facebook.

15. Defendant utilized the Pixel to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiffs' and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

16. The information that Defendant's Tracking Pixel sent to Facebook included the Private Information that Plaintiffs and Class Members submitted to Defendant's Website, including for example, the type of medical treatment sought, the individual's particular health condition and the fact that the individual attempted to or did book a medical appointment.

17. Such information allows a third party (*e.g.*, Facebook) to know that a specific

[3] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited March 8, 2023).

patient was confidentially seeking medical care. Facebook, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who geo-target Plaintiffs' and Class Members' Facebook pages based on communications obtained via the Facebook Pixel. Facebook and any third-party purchasers of Plaintiffs' and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia or HIV. Facebook and other third-party purchasers are thereby able to target and advertise to Plaintiffs and Class Members based on private, sensitive information they communicated to Defendant in confidence.

18. Covered entities such as Froedtert are simply ***not*** permitted to use these tracking technology tools in a way that exposes patients 'PHI to any third-party without prior, express and informed consent.

19. The Office for Civil Rights at the U.S. Department of Health and Human Services has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the unlawful transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals 'HIPAA-compliant authorizations, would constitute impermissible disclosures.***[4]

20. Such collection and dissemination of Private Information to third parties without the prior, informed consent of the Users violates federal and state law as well as Froedtert's Joint

[4] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited March 8, 2023) (emphasis added).

Notice of Privacy Practice and its Website Privacy Policy.[5]

21. Through the Pixel, Froedtert shares User's identities and online activity, including information and search results related to their private medical treatment. For example, upon visiting https://www.froedtert.com/doctors, patients can search for a doctor by Condition, Treatment, Specialty, Doctor or Location. When patients select a particular provider, this information is automatically sent to Facebook alongside the particular patient's Facebook identification ("FID").[6] Thus, the search parameters set by Users and Users 'FID number are shared together thereby allowing certain third-party recipients, here, Facebook, to make the direct connection between the search parameters and each individual Users 'FID.

22. Even absent an FID, other identifying information like IP addresses or device identifiers are captured by the Pixel and transmitted to Facebook.[7] The PHI Froedtert shares with Facebook during a patient's use of the appointment booking tool and "find a doctor" tool enables Facebook to identify what type health treatment each specific Froedtert patient is searching for, and Froedtert is sharing this information without its patients 'knowledge or informed consent.

23. Froedtert has publicly acknowledged the herein-described conduct. For instance (and as publicly reported), when a User accessed Froedtert's appointment scheduling web-page, "[c]licking the 'Schedule Online Now 'button for a doctor on the [Site] prompted the Facebook Pixel to send Facebook the text of the button, the doctor's name, and the condition we selected

[5] https://www.froedtert.com/patients-visitors/patient-privacy/privacy-practices; https://www.froedtert.com/website-privacy (last accessed March 8, 2023).

[6] An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone can look up a Users 'Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID so too can any person who comes into possession of an FID.

[7] Froedtert's doctor profile pages also contain a direct link that allows Users to call a particular doctor's office. When a patient clicks the phone call button, that information is immediately sent to Facebook and classified as a "SubscribeButtonClick."

from a dropdown menu: 'Alzheimer's.'"[8] And, when contacted about this violation of patient privacy, Froedtert, through a spokesperson, stated that it was removing the Pixel "out of an abundance of caution."[9]

24. Healthcare patients simply do not anticipate that their trusted healthcare provider will send personal health information or confidential medical information collected via its web pages to a hidden third party – let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue – without the patients 'consent.

25. Neither Plaintiffs nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook.

26. Despite willfully and intentionally incorporating the Facebook Pixel into its Website and servers, Defendant has never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook.

27. Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook as they communicated with their healthcare provider via the Website, or stored on Defendant's servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes.

28. Defendant owed common law, statutory and regulatory duties to keep Plaintiffs' and Class Members' communications and medical 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

[8] *See* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last accessed Oct. 24, 2022).
[9] *Id.*

to protect and to safeguard that information from unauthorized disclosure.

29. Froedtert breached its statutory and common law obligations to Plaintiffs and Class Members by, *inter alia*,: (i) failing to adequately review its marketing programs and web based technologies to ensure the its Web Properties were 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 written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through Facebook Pixels; (v) failing to warn Plaintiffs and Class Members and (vi) otherwise failing to design and to monitor its Web Properties to maintain the confidentiality and security of patient Private Information.

30. As a result, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the potential harms, (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information, (v) statutory damages and (v) the continued and ongoing risk to their Private Information.

31. Plaintiffs therefore bring, on behalf of themselves and a class of similarly situated persons, the following claims against Froedtert: (i) Invasion of Privacy, (ii) Unjust Enrichment; (iii) Breach of Confidence; (iv) Violation of Wisconsin's Confidentiality of Patient Health Care Records Act (Wis. Stat. § 146.81, *et seq.*); (v) violations of the Electronics Communication Privacy Act ("ECPA"), 18 U.S.C. § 2511(1) -unauthorized interception, use and disclosure; (vi) violations of ECPA, 18 U.S.C. § 2511(3)(a) -unauthorized interception, use and disclosure; (vii) violations of Title II of the ECPA, 18 U.S.C. § 2702, *et seq.* - Stored Communications Act and (viii) Violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030, *et seq.*).

PARTIES

32. Plaintiff KEEFE JOHN is a natural person and citizen of Wisconsin, residing at 1812 Pleasant Valley Rd. West Bend, WI 53095, Wisconsin, where he intends to remain.

33. Plaintiff JILLIAN CATHERINE KLUG is a natural person and citizen of Wisconsin, residing at 5758 N. River Forest Dr., Glendale, WI 53209, Wisconsin, where she intends to remain.

34. FROEDTERT HEALTH, INC. is a health care corporation operating a large regional network of hospitals (the "Network") with its principal place of business in Wauwatosa, Wisconsin. Froedtert's Network includes six hospitals in the State of Wisconsin.[10] In administering and providing health care services within its Network, Froedtert maintains a website (available at https://www.froedtert.com/) and a patient portal called MyChart. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d & 45 C.F.R. Part 160-45 C.F.R. Part 162, & 45 C.F.R. Part 164 ("HIPAA").

JURISDICTION & VENUE

35. This Court has personal jurisdiction over Defendant because its principal place of business is in this judicial district and a substantial portion of the acts and omissions giving rise to the claims asserted herein occurred in and emanated from this judicial district.

36. Venue is proper because Defendant's principal place of business is in this judicial district.

COMMON FACTUAL ALLEGATIONS

A. Background: The Use of Tracking Technologies in the Healthcare Industry.

37. Tracking tools installed on many hospitals', telehealth companies 'and other

[10] https://www.froedtert.com/locations (last visited March 8, 2023).

healthcare providers ’websites (and other digital properties) are collecting patients ’and other visitors ’confidential and private health information—including details about their medical conditions, prescriptions and appointments, among *many* other things—and sending that information to third party vendors without prior, informed consent.

38. These pixels are snippets of code that tracks users as they navigate through a website, logging which pages they visit, which buttons they click and certain information they enter into forms. In exchange for installing the pixels, the third-party platforms (*e.g.*, Facebook and Google) provide website owners analytics about the advertisements they have placed as well as tools to target Users who have visited their web properties.

39. While the information captured and disclosed without permission may vary depending on the pixel(s) embedded, these “data packets” can be extensive, sending, for example, not just the name of the physician and her field of medicine, but also the first name, the last name, email address, phone number and zip code and city of residence entered into the booking form.

40. That data is linked to a specific internet protocol (“IP”) address. The Meta Pixel, for example, sends information to Facebook via scripts running in a person’s internet browser so each data packet comes labeled with an IP address that can be used in combination with other data to identify an individual or household.

41. In addition, if the person is (or recently has) logged into Facebook when they visit a particular website when a Meta Pixel is installed, some browsers will attach third-party cookies—another tracking mechanism—that allow Meta to link pixel data to specific Facebook accounts.

42. Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals’, health care providers ’and telehealth companies ’digital properties to surreptitiously capture and to disclose their Users ’personal health

information ("PHI"). Specifically, and for example, The Markup reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment.[11]

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

43. Defendant purposely installed the Pixel and programmed its Website to surreptitiously share its patients 'Private Information with Facebook, including communications containing Plaintiffs' and Class Members' PHI and PII.

44. Further to the process described herein, Froedtert assisted Facebook with intercepting Plaintiff's communications including those that contained personally identifiable information, PHI and related confidential information.

45. Defendant assisted these interceptions without Plaintiffs 'knowledge, consent or express written authorization.

46. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiffs 'Private Information.

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

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

[11] *See, e.g.*, Tood Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited March 8, 2023).

C. Facebook's Business Tools & the Pixel

49. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[12]

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

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

52. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[13]

53. Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[14]

---

[12] 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 March 8, 2023).

[13] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Nov. 14, 2022); *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 March 8, 2023).

[14] 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 March 8, 2023).

54. One such Business Tool is the Pixel which "tracks the people and type of actions they take."[15]

55. When a user accesses a web page that is hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers—traveling from the user's browser to Facebook's server.

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

D. Defendant's method of transmitting Plaintiffs' & Class Members' Private Information via the Tracking Pixel (i.e., the interplay between HTTP Requests & Responses, Source Code & the Pixel)

57. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet.

58. Each "client device" (such as computer, tablet or smartphone) accessed web content through a web browser (*e.g.*, Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

59. 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.

60. 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.*,

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

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.[16]

63. A User'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 Website).

64. Every website consists of Markup and "Source Code."

65. Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

66. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user.

67. Defendant's Pixel is source code that does just that.

68. The Pixel acts much like a traditional wiretap.

69. When patients visit Defendant's website via an HTTP Request to Aspirus 'server,

[16] One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

that server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel.

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

71. 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.

E. Defendant's Pixel Tracking Practices caused Plaintiffs' & Class Members' Private Information to be sent to Facebook.

85. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel on its Website to secretly track patients by recording their activity and experiences in violation of its common law, contractual, statutory and regulatory duties and obligations.

86. Defendant's Web Pages contain a unique identifier which indicates that the Pixel is being used on a particular webpage.

87. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences and decrease advertising and marketing costs.

88. However, Defendant's Website does not rely on the Pixel in order to function. Indeed, numerous hospitals operate websites offering similar features to their patients without surreptitiously intercepting and sharing Private Information with third-parties.

89. While seeking and using Defendant's services as a medical provider, Plaintiffs and

Class Members communicated their Private Information to Defendant via its Website.

90. Defendant did not disclose to Plaintiffs and Class Members that their Private Information would be shared with Facebook as it was communicated to Defendant.

91. Plaintiffs and Class Members never consented, agreed, authorized or otherwise permitted Defendant to disclose their Private Information to Facebook nor did they intend for Facebook to be a party to their communications with Defendant.

92. Defendant's Pixel sent non-public Private Information to Facebook, including but not limited to Plaintiffs' and Class Members': (i) status as medical patients; (ii) health conditions; (iii) sought treatment or therapies; (iv) appointment requests and appointment booking information; (v) registration or enrollment in medical classes (such as breastfeeding courses); (vi) locations or facilities where treatment is sought; (vii) which web pages were viewed and (viii) phrases and search queries conducted via the general search bar.

93. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside Plaintiffs' and Class Members' Facebook ID (c_user cookie or "FID"), thereby allowing individual patients 'communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts.[17]

94. 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

[17] Defendant's Website tracks and transmits data via first-party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account and it is composed of a unique and persistent set of numbers.

Facebook profile.

95. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (i) implemented technology *(i.e.*, the Facebook Pixel) that surreptitiously tracked, recorded and disclosed Plaintiffs' and other online patients 'confidential communications and Private Information; (ii) disclosed patients 'protected information to Facebook—an unauthorized third-party and (iii) undertook this pattern of conduct without notifying Plaintiffs or Class Members and without obtaining their express written consent.

112. Plaintiffs never consented, agreed, authorized or otherwise permitted Defendant to disclose his personally identifiable information and protected health information nor did they authorize any assistance with intercepting their communications.

113. Plaintiffs were never provided with any written notice that Defendant disclosed its Website users 'protected health information nor were they provided any means of opting out of such disclosures.

114. Despite this, Defendant knowingly and intentionally disclosed Plaintiffs' PHI to Facebook.

115. By law, Plaintiffs are entitled to privacy in their protected health information and confidential communications.

116. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (i) implemented a system that surreptitiously tracked, recorded and disclosed Plaintiffs' and Class Members' confidential communications, personally identifiable information and protected health information to a third party; (ii) disclosed patients 'protected information to Facebook – an unauthorized third-party eavesdropper and (iii) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent.

G. Defendant's Privacy Policy & Promises

135. Froedtert's conduct violates its Joint Notice of Privacy Practice and Website Privacy Policy:

Our Pledge Regarding Your Protected Health Information

> Protected Health Information is any individually identifiable information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, or health care clearinghouse, and ***that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individua***l, or the past, present or future payment for the provision of health care to an individual, and ***that either identifies an individual (for example, an individual's name, social security number, or medical record number) or can reasonably be used to identify the individual (for example, your address, telephone number, or birth date).***
>
> We are committed to the privacy of your PHI, and we comply with applicable law and accreditation standards regarding patient privacy. PHI about you is personal. PHI may be in paper or electronic records but could also include photographs, videos and other electronic transmissions or recordings that are created during your care and treatment. A record of the care and services you receive is needed to provide you with quality care and to comply with legal requirements.
>
> ***The law requires us to:***
>
> - ***Make sure that PHI is kept private.***
> - Give you this Notice of our legal duties and privacy practices with respect to PHI about you.
> - ***Notify you in the event of a breach of your unsecured PHI.***
> - Follow the terms of this Notice that are currently in effect.[18]

136. Froedtert's Website Policy "outlines the information gathering and dissemination practices we follow and your rights as a user of our website" and **"**applies to all information we collect in the United States through our website [] including our mobile applications."[19]

137. Froedtert 'Policy does ***not*** disclose that it will collect and send PHI to a third party (such as Facebook):

[18] *See* https://www.froedtert.com/patients-visitors/patient-privacy/privacy-practices (listing acceptable "Uses and Disclosures" of PHI) (emphasis added).
[19] https://www.froedtert.com/website-privacy.

How We Use Your Personal Information

We recognize the importance of privacy. We do not sell or lease your personal information. We use your contact information to respond to your questions or to send you material and information you request, as well as to help us determine ways to restructure the website so it better serves you.

We may also use it to notify you of changes to our website or new services we think you may be interested in. You may elect not to receive these communications, either when you initially register as a member with our site or at any time thereafter.

We also use your website information in order to help identify problems with our website. We may use all information we collect to analyze statistical use patterns and demographic data, including where our visitors come from and what demographic characteristics they have and to improve our website to better serve our customers.

We participate in internet-based advertising. This means that we may use information about how you browse our website and others to help us improve our service offerings, websites and advertising.

Disclosing Your Personal Information to Others

We may share your personal information among our affiliates as necessary to provide you with the information and services you requested. ***Except in the limited circumstances listed, we do not provide unaffiliated third parties with personal information about our website visitors.***

These circumstances may include: - We may disclose information about you if and when we believe it is necessary to comply with any law, rule, or court order or subpoena; to enforce our legal rights or the rules of this website; or to protect our business, property and operations. - We may prepare and keep statistical records and other data about you and users of our site, but we do it in a way that does not identify you or any other user personally. - We may hire third parties to help us collect and analyze such data, and we may share such statistical data with third parties. ***Such statistical data will not specifically identify you or any other user.***

Asking Your Permission

It is our policy to always ask permission prior to retaining personal information or addresses of those using this website. Site features with high functionality often require that you register in order to access the feature and the information you have provided. In such cases, it is our policy to provide a mechanism that allows the user to opt out of the feature at any time in the future.[20]

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

138. Defendant's privacy policy does ***not*** permit it to use and to disclose Plaintiffs' and Class Members' Private Information for marketing purposes.

136. Defendant violated their own privacy policy by unlawfully intercepting and disclosing Plaintiffs' and Class Members' Private Information to Facebook and third parties without adequately disclosing that Defendant shared Private Information with third parties and without acquiring the Users 'consent or authorization to disclose the Private Information.

H. Federal Warning on Tracking Codes on Healthcare Websites.

137. Beyond Defendant's own policies, and those of Meta, the government has issued guidance warning that tracking code like Meta Pixel may come up against federal privacy law when installed on healthcare websites.

138. The statement, titled *Use of Online Tracking Technologies By HIPAA Covered Entities And Business Associates* (the "Bulletin"), was recently issued by the Department of Health and Human Services 'Office for Civil Rights ("OCR").[21]

139. Healthcare organizations regulated under the Health Insurance Portability and Accountability Act (HIPAA) may use third-party tracking tools, such as Google Analytics or Meta Pixel, in a limited way, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients 'protected health information to these vendors.

140. The Bulletin explains:

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

[21] HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaaonline-tracking/index.html (last visited March 8, 2023).

constitute impermissible disclosures.[22]

141. The bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.*** Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.*** While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***[23]

142. Plaintiffs and Class members face just the risks about which the government expresses concern. Defendant has passed along Plaintiffs' and Class Members' search terms about health conditions for which they seek doctors; their contacting of doctors to make appointments; the names of their doctors; the frequency with which they take steps relating to obtaining healthcare for certain conditions; and where they seek medical treatment.

143. This information is, as described by the OCR in its bulletin, "highly sensitive."

144. The Bulletin goes on to make clear how broad the government's view of protected information is as it explains:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code.***[24]

145. Crucially, that paragraph in the government's Bulletin continues:

> ***All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the***

[22] *Id.* (Emphasis added).
[23] *Id.* (emphasis added).
[24] *Id.* (emphasis added).

> ***IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.*** This is because, ***when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.***[25]

146. This is further evidence that the data that Defendant chose to share is protected Private Information; the sharing of which was a violation of Plaintiffs' and Class Members' rights.

I. Defendant's Violation of HIPAA.

147. Defendant's disclosure of Plaintiffs' and Class Members' Private Information to entities like Facebook also violated HIPAA.

148. HIPAA provided Plaintiffs and Class members with another reason to believe that the information they communicated to Defendant through its Web Properties would be protected, rather than shared with third-parties for marketing purposes.

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

150. HIPAA prohibits health care providers from "us[ing] or disclos[ing] 'protected health information 'except as permitted or required by" the HIPAA Privacy Rule. 45 C.F.R. § 164.502.

---

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

151. "A covered entity may determine that health information is not individually identifiable health information only if" either "a person with appropriate knowledge of and experience with generally accepted statistical and scientific methods for rendering information not individually identifiable: a) applying such principles" determines that the risk is "very small" that the information could be used alone, or in combination with other information, to identify individuals, and documents the methods that justifies such a determination, or identifiers are removed that include: Internet Protocol (IP) address numbers; account numbers; URLs, device identifiers, and "any other unique identifying number, characteristic or code," except codes assigned by the healthcare organization to allow itself to re-identify information from which it has removed identifying information.

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

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

> 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]

154. Consistent with this restriction, the HHS has issued marketing guidance that provides that: "[w]ith limited exceptions, the [Privacy] Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for

[26] HHS.gov, GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE, https://www.hhs.gov/hipaa/forprofessionals/privacy/special-topics/de-identification/index.html (last visited March 8, 2023).

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."[27]

155. Here, Defendant provided patient information to third parties in violation of this rule.

156. Commenting on a June 2022 report discussing the use of the Meta Pixel by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it…It is quite likely a HIPAA violation."[28]

157. Defendant's placing of the third-party tracking code on its Website is a violation of Plaintiffs' and Class Members' privacy rights under federal law. While Plaintiffs do not bring a claim under HIPAA itself, this violation evidences Defendant's wrongdoing as relevant to other claims.

J. Plaintiffs' & Class Members' Private Information Has Financial Value.

158. Plaintiffs' Private Information has economic value.

159. Indeed, Meta's, Google's and others' practices of using such information to package groups of people as "Lookalike Audiences" and similar groups and selling those packages to advertising clients demonstrates the financial worth of that data.

---

[27] HHS.gov, MARKETING, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html (last visited March 8, 2023).
[28] HHS.gov, Advisory Board, 'DEEPLY TROUBLED': SECURITY EXPERTS WORRY ABOUT FACEBOOK TRACKERS ON HOSPITAL SITES, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html (last visited March 8, 2023).

160. Data harvesting is the fastest growing industry in the nation.

161. As software, data mining and targeting technologies have advanced, the revenue from digital ads and the consequent value of the data used to target them have risen rapidly.

162. Consumer data is so valuable that some have proclaimed that data is the new oil.

163. Between 2016 and 2018, the value of information mined from Americans increased by 85% for Facebook and 40% for Google.

164. Overall, the value internet companies derive from Americans 'personal data increased almost 54%.

165. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user.

166. In 2022, that value is expected to be $200 billion industry wide, or $434 per user, also a conservative estimate.

167. As to health data specifically, as detailed in an article in Canada's National Post:

> As part of the multibillion-dollar worldwide data brokerage industry, health data is one of the most sought-after commodities. De-identified data can be re identified (citing https://www.nature.com/articles/s41467-019-10933-3/) and brazen decisions to release records with identifiable information (citing https://www.wsj.com/articles/hospitals-give-tech-giants-access-todetailed-medical-records-11579516200?mod=hp_lista_pos3) are becoming commonplace).[29]

168. Further demonstrating the financial value of Class Members 'medical data, CNBC has reported that hospital executives have received a growing number of bids for user data:

> Hospitals, many of which are increasingly in dire financial straits, are weighing a lucrative new opportunity: selling patient health information to tech companies. Aaron Miri is chief information officer at Dell Medical School and University of Texas Health in

[29] *See* National Post, IRIS KULBATSKI: THE DANGERS OF ELECTRONIC HEALTH RECORDS, February 26, 2020, https://nationalpost.com/opinion/iris-kulbatski-the-dangers-of-electronichealth-records (last visited March 8, 2023).

> Austin, so he gets plenty of tech start-ups approaching him to pitch deals and partnerships. Five years ago, he'd get about one pitch per quarter. But these days, with huge data-driven players like Amazon and Google making incursions into the health space, and venture money flooding into Silicon Valley start-ups aiming to bring machine learning to health care, the cadence is far more frequent. "It's all the time," he said via phone. "Often, once a day or more."
> * * *
> [H]ealth systems administrators say [the data] could also be used in unintended or harmful ways, like being cross-referenced with other data to identify individuals at higher risk of diseases and then raise their health premiums, or to target advertising to individuals.[30]

169. The CNBC article also explained:

> De-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers. Just one company alone, IQVIA, said on its website that it has access to more than 600 million patient records globally that are nonidentified, much of which it accesses through provider organizations. The buyers, which include pharma marketers, will often use it for things like clinical trial recruiting But hospital execs worry that this data may be used in unintended ways, and not always in the patient's best interest.
> * * *

170. Tech companies are also under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own needs. For instance, the health data Google collects could eventually help it micro-target advertisements to people with particular health conditions. Policymakers are proactively calling for a revision and potential upgrade of the health privacy rules known as HIPAA, out of concern for what might happen as tech companies continue to march into the medical sector.[31]

171. Time Magazine similarly, in an article titled, *How your Medical Data Fuels A*

[30] CNBC, HOSPITAL EXECS SAY THEY ARE GETTING FLOODED WITH REQUESTS FOR YOUR HEALTH DATA, https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-withrequests-for-your-health-data.html (last visited March 8, 2023).
[31] *Id.*

Hidden Multi-Billion Dollar Industry, referenced the "growth of the big health data bazaar," in which patients 'health information is sold. It reported that:

> [T]the secondary market in information unrelated to a patient's direct treatment poses growing risks, privacy experts say. That's because clues in anonymized patient dossiers make it possible for outsiders to determine your identity, especially as computing power advances in the future.[32]

172. Froedtert gave away Plaintiffs' and Class Members' communications and transactions on its Website without permission.

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

K. Defendant Violated Industry Standards.

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

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

176. AMA Code of Ethics Opinion 3.1.1 provides:

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

177. 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

[32] Time, HOW YOUR MEDICAL DATA FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY, https://time.com/4588104/medical-data-industry/ (last visited March 8, 2023).

> 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.

178. 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.[33]

L. Plaintiffs' & Class Members' Expectation of Privacy.

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

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

M. IP Addresses are Protected Health Information.

181. In addition to patient status, medical conditions, treatment, specific providers, appointment information and patient's unique and persistent Facebook ID, Defendant improperly disclosed Users' computer IP addresses to Facebook through the use of the Pixel. An IP address is a number that identifies the address of a device connected to the Internet.

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

183. IP addresses of individual Internet users are used by Internet service providers,

[33] https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf (last visited March 8, 2023).

Websites, and third-party tracking companies to facilitate and track Internet communications.

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

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

186. 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.

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

188. 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).

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

190. Consequently, Defendant's disclosure of patients 'IP addresses violated HIPAA and industry privacy standards.

N. Defendant was Enriched & Benefitted from the Use of The Pixel & Unauthorized Disclosures

191. The sole purpose of the use of the Facebook Pixel on Defendant's Website was marketing and profits.

192. In exchange for disclosing the Personal Information of its Users, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on Facebook.

193. Upon information and belief, Defendant was advertising its services on Facebook,

and the Pixel was used to "help [Defendant] understand the success of [its] advertisement efforts on Facebook."

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

195. Upon information and belief, Defendant re-targeted patients and potential patients to get more patients to use its services.

196. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

REPRESENTATIVE PLAINTIFFS 'EXPERIENCES

A. Plaintiff Keefe John

197. On numerous occasions and as a condition of receiving Defendant's services, with the most recent being in December 2022, Plaintiff John accessed Defendant's Website on his mobile device and computer and used the Website to look for providers at Froedtert, to arrange care and treatment to make appointments and to pay bills.

198. Plaintiff John scheduled doctor's appointments for himself via the Defendant's Website.

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

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

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

202. As described herein, Defendant worked along with Facebook to intercept Plaintiff John's communications, including those that contained Private Information.

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

204. Defendant transmitted to Facebook Plaintiff John's Facebook ID, computer IP address, and information such as appointment type, physician selected, button/menu selections, and/or content typed into free text boxes.

205. By doing so without Plaintiff John's consent, Defendant breached Plaintiff John's privacy and unlawfully disclosed his Private Information.

206. Defendant did not inform Plaintiff John that it had shared his Private Information with Facebook.

207. Plaintiff John suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs; (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 to his Private Information.

208. Plaintiff John has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

B. Plaintiff Jillian Catherine Klug

209. On numerous occasions and as a condition of receiving Defendant's services, with the most recent being in December 2022, Plaintiff Klug accessed Defendant's Website on her mobile device and computer and used the Website to look for providers at Froedtert, to arrange care and treatment to make appointments and to pay bills.

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

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

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

213. As described herein, Defendant worked along with Facebook to intercept Plaintiff Klug's communications, including those that contained her Private Information.

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

215. Defendant transmitted to Facebook Plaintiff Klug's Facebook ID, computer IP address, and information such as appointment type, physician selected, button/menu selections, and/or content typed into free text boxes.

216. Defendant did not inform Plaintiff Klug that it had shared her Private Information with Facebook.

217. Plaintiff Klug suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs; (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 to her Private Information.

218. Plaintiff Klug has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

TOLLING

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

CLASS ACTION ALLEGATIONS

220. As authorized by Wis. Stat. § 803.08, Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated (the "Class").

221. 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 a third party without authorization or consent through the Pixel on Defendant's Website.

222. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign and any Judge who adjudicates this case, including their staff and immediate family. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

223. **Numerosity:** The Nationwide Class members are so numerous that joining all members is impracticable. Upon information and belief, there are hundreds of thousands of individuals whose Private Information may have been improperly disclosed by Froedtert, and the Class is identifiable within Defendant's records.

224. **Commonality & Predominance:** Questions of law and fact common to the Classes 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 policy 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 it data security and/or privacy policy practices;

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

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

208. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of Defendant's use of the Facebook Pixel.

209. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be

antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

210. **Superiority and Manageability:** 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.

211. **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 Plaintiff.

212. 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 it would be able to exploit and to overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

213. 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.

214. **Ascertainability & Notice:** Membership in the Class can be determined by objective records maintained by Defendant and adequate notice can be given to Class Members directly using information maintained in Defendant's records.

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

216. Likewise, particular issues under Rule 23I(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 policy;

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.[34]

COUNT I
INVASION OF PRIVACY
(On Behalf of Plaintiffs & the Class)

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

218. Plaintiffs bring this claim individually and on behalf of the members of the

[34] Plaintiffs reserve the right to amend or modify the Class definition as this case progresses.

proposed Class against Defendant.

219. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Web Properties.

220. Plaintiffs and Class Members communicated sensitive and protected medical information and individually identifiable information that they intended for only Defendant to receive and that they understood Defendant would keep private.

221. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion.

222. Plaintiffs and Class Members had a reasonable expectation of privacy given Defendant's representations, HIPAA Notice of Privacy Practices and Privacy Policy.

223. Moreover, Plaintiffs and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

224. Defendant's disclosure of private medical information coupled with individually identifying information is highly offensive to the reasonable person.

225. As a result of Defendant's actions, Plaintiffs and Class Members have suffered harm and injury including, but not limited to, an invasion of their privacy rights.

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

227. Plaintiffs and Class Members seek appropriate relief for that injury including, but not limited to, damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as a result of its intrusions upon their privacy.

228. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights.

229. Such damages are needed to deter Defendant from engaging in such conduct in the future.

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

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

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

232. Defendant benefitted from Plaintiffs and Class Members and unjustly retained benefits at their expense.

233. 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.

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

235. 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.

236. The benefits that Defendant derived from Plaintiffs and Class Members was not

offered by Plaintiffs and Class Members gratuitously and rightly belongs to Plaintiffs and Class Members.

237. It would be inequitable under unjust enrichment principles in 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.

238. 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, as well as such other relief as the Court may deem just and proper.

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

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

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

241. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on its Website, which were further buttressed by Defendant's express promises in its privacy policy.

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

243. These disclosures were made without Plaintiffs' or Class Members 'knowledge,

consent, or authorization, and were unprivileged.

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

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

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

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

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

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

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

e. Nominal damages for each independent violation;

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

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

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

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

COUNT IV
VIOLATION OF CONFIDENTIALITY OF PATIENT HEALTH CARE RECORDS
Wis. Stat. § 146.81, *et seq*.

(On Behalf of Plaintiffs & the Class)

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

248. Under Wisconsin law, all patient health care records must remain confidential and patient health care records may only be released to a person upon the informed consent of the patient or as otherwise authorized by the patient.

249. Defendant disclosed the private and protected medical information of Plaintiffs and Class Members to unauthorized third parties without their knowledge, consent or authorization.

250. Froedtert is a healthcare provider as defined by Wis. Stat. Ann. § 146.816(1).

251. Plaintiffs and Class Members are patients and, as a healthcare provider, Defendant had and has an ongoing obligation not to disclose their Private Information.

252. The Private information disclosed by Defendant is PHI as defined by Wis. Stat. Ann. § 146.816(f).

253. Defendant violated Wis. Stat. § 146.81, *et seq*., through its willful and knowing failure to maintain and to preserve the confidentiality of the medical information of Plaintiffs and the Class Members.

254. Defendant's conduct with respect to the disclosure of its patients 'confidential Private Information was willful and knowing because it configured and implemented the digital platforms and tracking software that gave rise to sharing its User's Private Information (PII and PHI) with third parties.

255. Plaintiffs and Class Members were injured as a result of Defendant's violation of the confidentiality of patient health care law.

256. As a result of its intentional and willful disclosure of Plaintiffs' and Class

Members' Private Information, Defendant is liable for actual damages, additional damages of at least $25,000 if the violation was willful or $1,000 otherwise and the costs and attorneys 'fees incurred as a result of the violation. *See* Wis. Sta. Ann. § 146.84.

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 & the Class)

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

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

259. 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.

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

261. **Electronic Communications**. The transmission of PII and PHI between Plaintiffs and Class Members and Defendant's 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 photo optical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

262. **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." *See* 18 U.S.C. § 2510(8).

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

264. **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).

265. 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;

d. Defendant's Website and

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

260. 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).

261. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the Pixel, which tracked, stored and unlawfully disclosed Plaintiffs' and Class Members' Private Information to Facebook.

262. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs' and Class Members' regarding Private Information, treatment, medication and scheduling.

263. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to 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).

264. 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).

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

266. Defendant intentionally used the wire or electronic communications to increase its profit margins.

267. Defendant specifically used the Pixel to track and to utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

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

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

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

271. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of its Website, Defendant's purpose was tortious, criminal and designed to violate federal and state legal provisions, including as described above the following: (i) a knowing intrusion into a private, place, conversation or matter that would be highly offensive to a reasonable person; and (ii) violation of Wis. Stat. § 146.81, *et seq*.

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

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

273. The ECPA 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).

274. **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).

275. Defendant's Website is an electronic communication service which provides to 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.

276. **Intentional Divulgence**. Defendant intentionally designed the Pixel tracking and was or should have been aware that, if so configured, it could divulge Plaintiffs' and Class Members' Private Information.

277. **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.

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

279. **Exceptions do not apply**. In addition to the exception for communications directly to an electronic communications service ("ECS")[35] or an agent of an ECS, the ECPA states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication."

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."

U.S.C. § 2511(3)(b).

[35] An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

279. 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.

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

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

282. Defendant's divulgence of the contents of user communications on its Website 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: (i) Plaintiffs and Class Members did not authorize Defendant to divulge the contents of their communications and (ii) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiffs and Class Members were exchanging information.

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

284. 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.

285. 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 & the Class)

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

287. 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).

288. **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).

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

290. **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).

291. Defendant stores the content of Plaintiffs' and Class Members' communications on Defendant's Website and files associated with it.

292. When Plaintiffs or Class Members make a Website communication, the content of that communication is immediately placed into storage.

293. Defendant knowingly divulges the contents of Plaintiffs' and Class Members' communications through the Pixel.

294. **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 a 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."

295. 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.

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

297. 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.

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

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

300. Defendant's divulgence of the contents of user communications on its Website was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (i) Plaintiffs and Class Members did not authorize

Defendant to divulge the contents of their communications and (ii) Defendant did not procure the "lawful consent" from the websites or apps with which Plaintiffs and Class Members were exchanging information.

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

302. 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.

303. 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 & the Class)

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

305. Plaintiffs' and the Class Members '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).

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

307. Defendant's conduct 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 Members '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.

308. 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 and personally identifiable data and content of Plaintiffs and the Class Members 'Website Communications being made available to Defendant, Facebook, and/or other third parties without adequate legal privacy protections.

309. Accordingly, Plaintiffs and the Class Members 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).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Keefe John and Jillian Catherine Klug respectfully pray for judgment in their favor and against Defendant Froedtert Health, Inc. as follows:

- For an Order certifying this action as a class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;
- For equitable relief enjoining Defendant from disclosing Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;
- For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage and safety, and to disclose with specificity the type of PII

and PHI disclosed to third parties;

- For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

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

- For an award of punitive damages as allowable by law;

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

- Pre- and post-judgment interest on any amounts awarded and

- All such other and further relief as this court may deem equitable and just.

DEMAND FOR JURY TRIAL

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

Date: March 16, 2023.

Respectfully submitted,

HANSEN REYNOLDS LLC

/s/ Timothy M. Hansen
Timothy M. Hansen (SBN 1044430)
301 N. Broadway, Suite 400
Milwaukee, Wisconsin 53202
(414) 455-7676 (phone)
(414) 273-8476 (fax)
thansen@hansenreynolds.com

ALMEIDA LAW GROUP LLC

David S. Almeida (SBN 1086050)
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024 (phone)
david@almeidalawgroup.com

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

Gary M. Klinger
227 Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

Attorneys for Plaintiffs & the Proposed Class