COPY

EFILED 11/25/24 03:37 PM CASE NO. 23C2513 Joseph P. Day, Clerk

IN THE CIRCUIT COURT FOR THE TWENTIETH JUDICIAL DISTRICT,
DAVIDSON COUNTY, TENNESSEE
AT NASHVILLE

JANE DOE, Individually, and as Mother and Next Friend of J.D., a Minor, and ANITA AUGUSTY, PATRICIA BALL, JAMIE BARRY, EFFIE CARTER, EVITA COOPER, DEMORRIS GEAR, DAWN HARPER, BARBARA JANSSEN, TONYA LYNN JOHNSON, TAMMIE KNIGHT, ROBERTA MALONE SHAY, SUMMER MCDONALD, ZACHARY MAXWELL, SHAREE PEACOCK, KEVIN PRESCOTT, DENNY RANDALL, CHERYL RHOADES, LAURA SHELTON, JAMES SHEWEY, ALYSSA SWETLOCK, BETTY BOGARD, and TINA TUCKER, on behalf of themselves all others similarly situated,	)	
Plaintiffs,	)	
v.	)	
HSCGP, LLC	)	
Defendant.	)	

FIRST AMENDED CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiffs , Jane Doe, individually, and as Mother and Next Friend of J.D., a Minor, and Anita Augusty, Patricia Ball, Jamie Barry, Effie Carter, Evita Cooper, Demorris Gear, Dawn Harper, Barbara Janssen, Tonya Lynn Johnson, Tammie Knight, Roberta Malone Shay, Summer McDonald, Zachary Maxwell, Sharee Peacock, Kevin Prescott, Denny Randall, Cheryl Rhoades, Laura Shelton, James Shewey, Alyssa Swetlock, Betty Bogard, and Tina Tucker, on behalf of themselves and all others similarly situated (hereinafter "Plaintiffs") bring this Class Action Complaint against Defendant, HSCGP, LLC (hereinafter "HSCGP" or "Defendant"), and allege,

COPY

upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Defendant manages the unauthenticated, public websites ("Websites") of a number of healthcare companies ("Serviced Companies"). Plaintiffs bring this class action to address Defendant's improper practice of managing the Websites of Serviced Companies so as to disclose the confidential Personally Identifying Information ("PII")[1] and/or Protected Health Information ("PHI")[2] (collectively referred to as "Private Information") of Plaintiffs and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"),[3] and potentially others ("the Disclosure") via tracking technologies used on its website.

2. The Office for Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS") and the Federal Trade Commission ("FTC") warn about the "serious privacy and security risks related to the use of online tracking technologies" present on websites or online platforms, such as those managed by Defendant, that "impermissibly disclos[e] consumers'

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). WCCH is clearly a "covered entity" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

[3] Facebook changed its name from Facebook, Inc. to Meta Platforms, Inc. in October 2021. Plaintiff's reference to both "Facebook" and "Meta" throughout this complaint refer to the same company.

COPY

sensitive personal health information to third parties."[4] OCR and FTC agree that such tracking technologies, like those present on the websites managed by Defendant, "can track a user's online activities" and "gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users."[5] OCR and FTC warn that "[i]mpermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information 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."[6]

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

4. Recognizing these facts, and in order to implement requirements of the Health

[4] U.S. Dep't of Health & Human Services, *Re: Use of Online Tracking Technologies*, (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf, **attached as Exhibit A.**
[5] *Id.*
[6] *Id.*

COPY

Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

5. Serviced Companies include Acquisition Bell Hospital, LLC, Ashley Valley Medical Center, LLC, Athens Regional Medical Center, LLC, Bourbon Community Hospital, LLC, Castleview Hospital, LLC, Clinch Valley Medical Center, Inc., Crockett Hospital, LLC, Danville Regional Medical Center, LLC, DLP Central Carolina Medical Center, LLC, DLP Conemaugh Memorial Medical Center, LLC, DLP Conemaugh Meyersdale Medical Center, LLC, DLP Conemaugh Miners Medical Center, LLC, DLP Frye Regional Medical Center, LLC, DLP Harris Regional Hospital, LLC, DLP Haywood Regional Medical Center, LLC, DLP Maria Parham Medical Center, LLC, DLP Marquette General Hospital, LLC, DLP Person Memorial Hospital, LLC, DLP Rutherford Regional Health System, LLC, DLP Swain County Hospital, LLC, DLP Twin County Regional Healthcare, LLC, DLP Wilson Medical Center, LLC, Essent PRMC, L.P., Fauquier Medical Center, LLC, Fleming Medical Center, LLC, Georgetown Community Hospital, LLC, Havasu Regional Medical Center, LLC, Hillside Hospital, LLC, Hot Springs National Park Hospital Holdings, LLC, Kentucky Hospital, LLC, Lake Cumberland Regional Hospital, LLC, Lourdes Hospital, LLC, Meadowview Regional Medical Center, LLC, Nason Medical Center, LLC, Norton Scott Hospital LLC d/b/a Norton Scott Hospital, Norton Clark Hospital LLC d/b/a Norton Clark Hospital, PHC-Elko, Inc., PHC-Fort Mohave, Inc., PHC-Las Cruces, Inc., PHC-Los Alamos, Inc., PineLake Regional Hospital, LLC, Portage Hospital, LLC, Raleigh General Hospital, LLC, RCCH Trios Health, LLC, RCHP - Florence, LLC, RCHP

COPY

- Ottumwa, LLC, RCHP Billings - Missoula, LLC, RCHP-Sierra Vista, Inc., Riverview Medical Center, LLC, Russellville Holdings, LLC, Saline Hospital, LLC, Southern Tennessee Medical Center, LLC, Spring View Hospital, LLC, Sumner Regional Medical Center, LLC, Trousdale Medical Center, LLC, Willamette Valley Medical Center, LLC, Woodford Hospital, LLC, and Wythe County Community Hospital, LLC (collectively, the "Serviced Companies").

6. Despite the unique position of Serviced Companies as trusted healthcare providers, Defendant knowingly configured and implemented into their Websites, code-based tracking devices known as "pixels" (also referred to as "trackers" or "tracking technologies"), which collected and transmitted patients' Private Information to Facebook and other third parties, without patients' knowledge or authorization.

7. Serviced Companies encouraged patients to use the Websites, along with secure online websites that gives patients access to records that contain protected health information ("Patient Portals"), to find a doctor, search for treatment services, schedule appointments, access patient portal pages through a "pre-portal" login page, pay bills, and more.

8. When Plaintiffs and the Class Members used the Websites and Patient Portals, they thought they were communicating exclusively with their trusted healthcare provider. Unbeknownst to them, Defendant embedded pixels from Facebook, and others into the Websites and Patient Portals, surreptitiously forcing Plaintiffs and Class Members to transmit intimate details about their medical treatment to third parties without their consent.

9. A pixel (also referred to as a "tracker" or "tracking technology") is a snippet of code embedded into a website that tracks information about its visitors and their website interactions.[7] When a person visits a website with an embedded pixel, the pixel tracks "events"

[7] *See* Meta, *Meta Pixel*, META, https://developers.facebook.com/docs/meta-pixel/ (last accessed Nov. 20, 2024).).

COPY

(i.e., user interactions with the site), such as pages viewed, buttons clicked, and information submitted.[8] Then, the pixel transmits the event information back to the website server and to third parties, where it can be combined with other data and used for marketing.[9]

10. Among the trackers Defendant embedded into the Websites is the Facebook Pixel (also referred to as the "Meta Pixel" or "Pixel"). By default, the Meta Pixel tracks information about a visitor's device, including their IP address, and the pages viewed.[10] When configured to do so, the Meta Pixel can track much more, including a visitor's search terms, button clicks, and form submissions.[11] Additionally, the Meta Pixel can link a visitor's website interactions with an individual's unique and persistent Facebook ID ("FID"), allowing a user's health information to be linked with their Facebook profile.[12]

11. Operating as designed and as implemented by Defendant, the Meta Pixel allowed Defendant to unlawfully disclose Plaintiffs and Class Members' Private Health Information alongside identifying details to Facebook. By installing the Meta Pixel on the Websites, Defendant effectively planted a bug on Plaintiffs' and Class Members' web browsers and compelled them to disclose Private Information and confidential communications to Facebook without their authorization or knowledge.

12. Facebook encourages and recommends use of its Conversions Application

---

[8] *See* Meta, *Conversion Tracking*, META, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited Nov. 20, 2024).
[9] *Id.*
[10] *See* Get Started, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/get-started (last visited May 22, 2023).
[11] *See* Conversion Tracking, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking (last visited May 22, 2023).
[12] The Meta Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." What are Cookies?, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

COPY

Programming Interface ("CAPI") alongside use of the Meta Pixel.[13]

13. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[14, 15]

14. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[16]

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

16. Defendant utilized data from these trackers to market its services and bolster its profits. Meta Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiffs' and Class Members' Private Information to create targeted advertisements based on the medical

---

[13] "CAPI works with your Meta Pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir El Kamouny, How to Implement Facebook Conversions API (In Shopify), FETCH & FUNNEL, https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Nov. 25, 2024).

[14] What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last updated May 20, 2022).

[15] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." Conversions API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/conversions-api (last visited May 15, 2023).

[16] About Conversions API, META FOR DEVELOPERS, https://www.facebook.com/business/help/2041148702652965 (last visited Nov. 25, 2024).

COPY

conditions and other information disclosed the Serviced Companies.

17. The information that Defendant-managed Websites' Meta Pixel and possibly CAPI sent to Facebook can include the Private Information that Plaintiffs and Class Members submitted to the Serviced Companies' Websites, including, for example, the contents of their search queries for services, the parameters of their doctor searches, information regarding scheduling appointments, information attendant to logging into a patient portal, and the buttons that they clicked.

18. Such information allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers, who then geotarget Plaintiffs' and Class Members' Facebook pages based on communications obtained via the Meta Pixel and CAPI. Facebook and any third-party purchasers of Plaintiffs' and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

19. In addition to the Facebook tracker and CAPI, Defendant installed other tracking technology, including on information and belief, Google Analytics, and others. On information and belief, these trackers operate similarly to the Meta Pixel and transmit a website user's Private Information to other third parties.

20. Healthcare patients simply do not anticipate that their trusted healthcare provider will send Personal Health Information or other confidential medical information collected via its webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patients' consent.

21. Neither Plaintiffs nor any Class Member signed a written authorization permitting

COPY

Defendant or the Serviced Companies to send their Private Information to Facebook, Google, or any other third parties uninvolved in their treatment.

22. Despite willfully and intentionally incorporating tracking technology, including the Meta Pixel, potentially CAPI, and other tracking technology, into the Websites and servers, neither Defendant nor the Serviced Companies disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with third parties including Facebook, and possibly Google, and others, until June 13, 2023, in an update to its Websites Privacy Policy.[17]

23. The Serviced Companies further made express and implied promises to protect Plaintiffs' and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with the Serviced Companies. Defendant, in managing the Websites, was also bound by these promises.

24. Defendant owed common law, statutory, and regulatory duties to keep Plaintiffs' and Class Members' communications and Private Information safe, secure, and confidential.

25. Upon information and belief, Defendant utilized the Meta Pixel and other tracker data to improve and to save costs on its marketing campaigns, improve its data analytics, attract new patients, and generate sales.

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

27. Defendant breached its statutory and common law obligations to Plaintiffs and

[17] *See* Wythe Cnty. Cmty. Hosp., *Web Privacy Policy* (June 2, 2023) (acc. via the Wayback Machine), https://web.archive.org/web/20230602015515/https://www.wcch.org/privacy-policy (last acc. Sept. 5, 2023), **attached as Exhibit B;** Wythe Cnty. Cmty. Hosp., *Web Privacy Policy*, (as rev. June 13, 2023), https://www.wcch.org/privacy-policy (last visited Nov. 25, 2024), **attached as Exhibit C.**

COPY

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

28. Plaintiffs seek to remedy these harms and bring causes of action for (I) Negligence; (II) Negligence *Per Se*; (III) Invasion of Privacy, Intrusion Upon Seclusion; (IV) Breach of Implied Contract; (V) Unjust Enrichment; (VI) Breach of Fiduciary Duty; (VII) Violation of the Tennessee Consumer Protection Act, Tenn. Code Ann. § 47-18-101, *et seq.*, and the similar consumer protection laws of other states; and (VIII) Violation of Tenn. Code Ann. § 39-13-601, *et seq.*, and the similar wiretap laws of the United States and other states.

PARTIES

29. Plaintiffs, Jane Doe, individually, and as Mother and Next Friend of J.D., a Minor, and Anita Augusty, Patricia Ball, Jamie Barry, Effie Carter, Evita Cooper, Demorris Gear, Dawn Harper, Barbara Janssen, Tonya Lynn Johnson, Tammie Knight, Roberta Malone Shay, Summer McDonald, Zachary Maxwell, Sharee Peacock, Kevin Prescott, Denny Randall, Cheryl Rhoades, Laura Shelton, James Shewey, Alyssa Swetlock, Betty Bogard, and Tina Tucker, are natural persons and are patients of Serviced Companies and victims of HSCGP's management of the

COPY

Serviced Companies' Websites.

30. Defendant, on behalf of the Serviced Companies, controlled the use, configuration, and design of the Meta Pixel and other online tracking technologies such that the Serviced Companies did not individually determine whether and how to use such technologies independent of HSCGP.

JURISDICTION AND VENUE

31. This Court has general jurisdiction over this action under T.C.A. § 16-10-101.

32. This Court has general personal jurisdiction over Defendant because the ownership of its LLC is in Davidson County, and the conduct at-issue occurred in Tennessee.

33. Venue is proper in this County under T.C.A. § 20-4-101 because the cause of action arose in this county and Defendant resides or is found in this county.

COMMON FACTUAL ALLEGATIONS

A. Background

34. The Serviced Companies serve many patients via the Websites and Patient Portals, which encourage patients to use to find doctors and other providers, search for and research medical services, schedule appointments, access patient portal pages through a "pre-portal" login page, pay bills, and more. Defendant and the Serviced Companies promote the comprehensive functionality of these tools and promote their use, in service of the own goal of increasing profitability.

35. In furtherance of the goal of increasing sales and profitability, and to improve the success of advertising and marketing, Defendant purposely installed the Meta Pixel and other trackers onto the Websites, for the purpose of gathering information about Plaintiffs and Class Members to further marketing efforts. But Defendant did not only generate information for their

COPY

own use: they also shared patient information, including Private Information belonging to Plaintiffs and Class Members, with Facebook and other unauthorized third parties.

36. To better understand Defendant's unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows.

i. Facebook's Business Tools and the Meta Pixel

37. 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.[18]

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

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

40. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[19] Businesses that want to target customers and advertise their services, such as Defendant and the Serviced Companies, can track

[18] Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022).

[19] Specifications for Facebook Pixel Standard Events, META, https://www.facebook.com/business/help/402791146561655 (last visited Jan. 31, 2023); *see also* Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS; https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* Best Practices for Facebook Pixel Setup, META https://www.facebook.com/business/help/218844828315224; App Events API, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Nov. 20, 2024).

COPY

other user actions and can create their own tracking parameters by building a "custom event."[20]

41. One such Business Tool is the Meta Pixel, a tool that "tracks the people and type of actions they take."[21] When a user accesses a webpage that is hosting the Meta Pixel, the communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook—traveling from the user's browser to Facebook's server.

42. Notably, this transmission only occurs on webpages that contain the Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate patient privacy (such as the homepage) and disable it on pages that do implicate patient privacy (such as Serviced Companies' "Find a Doctor" and "Schedule Appointment Now" page).

43. The Meta Pixel's primary purpose is for marketing and ad targeting and sales generation.[22]

44. Facebook's own website informs companies that "[t]he Meta Pixel is a piece of code that you put on your website that allows you to measure the effectiveness of your advertising by understanding the actions people take on your website."[23]

45. According to Facebook, the Meta Pixel can collect the following data.

> **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and ***person using the website.*** (emphasis added).
>
> **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.
>
> **Button Click Data** – Includes any buttons clicked by site visitors, the labels those buttons and any pages visited as a result of the button clicks.

---

[20] Meta Business Help Ctr., *About Standard and Custom Website Events*, META, https://www.facebook.com/business/help/964258670337005; *see also* Facebook, App Events API, *supra*.
[21] Retargeting, META, https://www.facebook.com/business/goals/retargeting.
[22] *See Meta Pixel*, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Nov. 20, 2024).
[23] Meta Business Help Ctr., *About Meta Pixel*, META, https://www.facebook.com/business/help/742478679120153 (last accessed Nov. 20, 2024).

COPY

> **Optional Values** – Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Example custom data events are conversion value, page type and more.
>
> **Form Field Names** – Includes website field names like email, address, quantity, etc., for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching or optional values.[24]

46. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- **Make sure your ads are shown to the right people.** Find new customers, or people who have visited a specific page or taken a desired action on your website.

- **Drive more sales**. Set up automatic bidding to reach people who are more likely to take an action you care about, like making a purchase.
- **Measure the results of your ads.** Better understand the impact of your ads by measuring what happens when people see them.[25]

47. Facebook likewise benefits from the data received from the Meta Pixel and uses the data to serve targeted ads and identify users to be included in such targeted ads.

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

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

49. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users'

[24] Meta Pixel, META FOR DEVELOPERS, https://developers.facebook.com/docs/meta-pixel/ (last accessed Nov. 20, 2024).
[25] About Meta Pixel, META, https://www.facebook.com/business/help/742478679120153 (last accessed Nov. 20, 2024).

COPY

client devices via their web browsers.

50. 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.[26]

51. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), they also send the host server data, which is embedded inside the URL and can include cookies.

52. When an individual visits a website, their web browser sends an HTTP Request to the entity's servers that essentially asks the website to retrieve certain information (Serviced Companies' "Find a Doctor" page). The entity's servers send the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate a website.

53. Every website is comprised of Markup and "Source Code." 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.

54. 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.

55. Defendant's implementation of the Meta Pixel is source code that acted much like a traditional wiretap, intercepting and transmitting communications intended only for Serviced Companies.

[26]"Cookies are small files of information that a web server generates and sends to a web browser . . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Jan. 27, 2023).

COPY

56. Separate from the Meta Pixel, Facebook and other website owners can place third-party cookies in the web browsers of users logged into their websites or services. These cookies can uniquely identify the user so the cookie owner can track the user as she moves around the internet—whether on the cookie owner's website or not. Facebook uses this type of third-party cookie when Facebook account holders use the Facebook app or website. As a result, when a Facebook account holder uses Defendant -managed Websites, the account holder's unique Facebook ID is sent to Facebook, along with the intercepted communication, allowing Facebook to identify the patient associated with the Private Information it has intercepted.

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

58. Conversions API "is designed to create a direct connection between [web hosts'] marketing data and [Facebook]."[27] Thus, the entity receives and stores its communications with patients on its server before Conversions API collects and sends those communications—and the Private Information contained therein—to Facebook.

59. Notably, client devices do not have access to host servers and thus cannot prevent (or even detect) this additional transmission of information to Facebook.

60. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the host server, Facebook instructs companies to "[u]se the

[27] Meta Business Help Ctr., *About Conversions API,* META, https://www.facebook.com/business/help/2041148702652965 (last visited Nov. 20, 2024).

COPY

Conversions API in addition to the Meta Pixel, and share the same events using both tools," because such a "redundant event setup" allows the entity "to share website events [with Facebook] that the pixel may lose."[28] Thus, if an entity implemented the Meta Pixel in accordance with Facebook's documentation, it is also reasonable to infer that it implemented the Conversions API tool on its Websites.

61. The third parties to whom a website transmits data through pixels and other tracking technology do not provide any substantive content on the host website. In other words, Facebook and others like it are not providing anything to the user relating to the user's communications. Instead, these third parties are typically procured to track user data and communications only to serve the marketing purposes of the website owner (i.e., to bolster profits).

62. Accordingly, without any knowledge, authorization, or action by a user, a website manager like Defendant can use its source code to commandeer patients' computing devices, causing the device's web browser to contemporaneously and invisibly re-direct the patients' communications to hidden third parties like Facebook.

63. In this case, Defendant employed the Meta Pixel and potentially Conversions API to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to Facebook contemporaneously, invisibly, and without the patient's knowledge.

64. Consequently, when Plaintiffs and Class Members visited Defendant -managed Websites and communicated their Private Information, it was simultaneously intercepted and transmitted to Facebook.

65. Defendant also employed other trackers, including from Google, and likely others, which, on information and belief, likewise transmitted Plaintiffs' and the Class Members' Private

[28] *See* Meta Business Help Ctr., *Best Practices for Conversions API*, META, https://www.facebook.com/business/help/308855623839366 (last visited Nov. 20, 2024).

COPY

Information to third parties without Plaintiffs' and Class Members' knowledge or authorization.

iii. HSCGP Violated the Privacy Policies of Serviced Companies

66. Serviced Companies are covered under a Notice of Privacy Practices,[29] and website privacy policies,[30] which are posted and maintained on Serviced Companies' Websites ("Privacy Policies").

67. Serviced Companies' Notice of Privacy Practices provide, for example, that, "[t]his notice describes how medical information about you may be used and disclosed and how you can get access to this information. PLEASE REVIEW THIS INFORMATION CAREFULLY. This notice applies to Wythe County Community Hospital and the doctors and other healthcare providers practicing at this facility."[31]

68. Serviced Companies' Notice of Privacy Practices goes onto acknowledge, represent, and promise patients that:

> It is our legal duty to protect the privacy and security of your information. **We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.** We are providing this notice so that we can explain our privacy practices. We must follow the duties and privacy practices described in this notice or the current notice in effect.[32]

69. In its Notice of Privacy Practices, Serviced Companies further represents and promises patients, for example, that it, "…**will never share your information unless you give us written permission in these cases: for marketing purposes or the sale of your information."**[33]

---

[29] *See, e.g.*, Wythe Cnty. Cmty. Hosp., *Notice of Privacy Practices* (Oct. 15, 2018), https://www.wcch.org/wythe-notice-of-privacy-practices, **Exhibit D.**
[30] *See, e.g.*, Wythe Cnty. Cmty. Hosp., *Privacy Policy*, (June 2, 2023), acc. via the Wayback Machine, https://web.archive.org/web/20230602015515/https://www.wcch.org/privacy-policy, **Exhibit B;** and Wythe Cnty. Cmty. Hosp., *Web Privacy Policy*, (as rev. June 13, 2023), https://www.wcch.org/privacy-policy, **Exhibit C.**
[31] Wythe Cnty. Cmty. Hosp.. *Notice of Privacy Practices*, **Exhibit D.**
[32] *Id*. (emphasis added).
[33] *Id*. (emphasis added).

COPY

70. In addition, in the Notice of Privacy Practices, Serviced Companies provide certain enumerated purposes for which it may disclose Private Information and PHI, for example, including: "cases of abuse, neglect, or other reasons requiring law enforcement; for public health activities; to health oversight agencies; for judicial and administrative proceedings; for death and funeral arrangements; for organ donation; for special government functions including military and veteran requests and to prevent serious threats to health or public safety such as preventing disease, helping with product recalls, and reporting adverse reactions to medications[,]" as well as for appointment reminders, treatment alternatives, or other health services.[34]

71. Serviced Companies go onto state in its Notice of Privacy Practices, for example, that, "[w]e will obtain your written authorization for any other disclosures beyond the reasons listed above."[35]

72. Via the Meta Pixel and other tracking technology, HSCGP unauthorizedly disclosed the PHI and Private Information of Plaintiffs and the Class Members without their written authorization in violation of Serviced Companies' Notice of Privacy Practices.

73. Further, Serviced Companies maintain website privacy policies, for example, the Public Online Privacy Policy in effect as of June 2, 2023 ("Websites Privacy Policy," Exhibit B), and revised as of June 13, 2023 ("June 13, 2023 Web Privacy Policy," Exhibit C).[36]

74. Serviced Companies' Websites Privacy Policy stated, for example:

> **Your privacy is important to us.** This Public Online Privacy Policy and the links included explain how we collect, treat, and protect your individually identifiable personal information. Specifically, the Public Online Privacy Statement describes how we handle the personal information that you submit to us when you submit a Contact Us form, attach

[34] *Id*.
[35] *Id*.
[36] Wythe Cnty. Cmty. Hosp., *Website Privacy Policy*, (June 2, 2023), acc. via the Wayback Machine, https://web.archive.org/web/20230602015515/https://www.wcch.org/privacy-policy (last acc. Sept. 5, 2023), **Exhibit B;** and Wythe Cnty. Cmty. Hosp., *Web Privacy Policy*, (as rev. June 13, 2023), https://www.wcch.org/privacy-policy, **Exhibit C.**

COPY

a resume, and browse our website.[37]

75. Serviced Companies' Websites Privacy Policy explained, for example, that it, "…designed [its] public websites to capture two types of information: automatic tracking and individually identifiable personal information ("personal information"). The first allows [it] to see which topics interest you most; the second helps [HSCGP and the Serviced Companies] provide the services you requested."[38]

76. In the Websites Privacy Policy, Serviced Companies acknowledged, represented and promised, for example, that:

> - We will only use the information to provide you with the services you have requested and as otherwise described in this Public Online Privacy Policy
> - We will NOT sell, rent, or license the personal information you provide within our public websites.
> - We do NOT provide any personally identifiable information about our users to any third party.
> - Access to the data you submit is limited to the authorized staff detailed in our Site Disclaimer under Security.
>
> [39]

77. The Websites Privacy Policy admitted, for example, that Serviced Companies' Websites used "'cookies' to personalize our site for you and to collect aggregate information about site usage by all of our users […but that…] [it] does not contain information that would personally identify you."[40]

78. Via the Meta Pixel and other tracking technology, HSCGP unauthorizedly disclosed the PHI and Private Information of Plaintiffs and the Class Members without their

[37] Wythe Cnty. Cmty. Hosp., *Web Privacy Policy*, (June 2, 2023), acc. via the Wayback Machine, https://web.archive.org/web/20230602015515/https://www.wcch.org/privacy-policy, **Exhibit B**.
[38] *Id*.
[39] *Id*.
[40] *Id*.

COPY

written authorization in violation of the Websites Privacy Policy.[41]

79. On or about June 13, 2023, Serviced Companies revised one of the Websites Privacy Policies in the June 13, 2023, Web Policy (Ex. C), where Serviced Companies stated, for example, that: "**Data Security** We are committed to protecting the privacy of the personal information you provide to us via this website so that we can make sure it remains as secure as possible."[42]

80. Serviced Companies' revised June 13, 2023, Web Privacy Policy disclosed and admitted, for example, its use of trackers such as the Meta Pixel, stating:

> This website works with companies that offer third-party products or services ("Service Providers"). These include Facebook, Google, and other Service Providers who help us track and analyze visitor activity on the website, measure the effectiveness of our advertising efforts, and support the optimization of our digital marketing campaigns.
>
> The website uses "cookies," tracking pixels and related technologies. These can be set by us or by our Service Providers. [43]

81. Further, the June 13, 2023, Web Privacy Policy explained, for example, that:

> Our Service Providers may acquire additional information about your activity on our website, including pages you visit, access times, visit duration, how you arrived at our website and your IP address. An IP address is a number that identifies a device connected to the Internet. For most devices, the IP address changes on at least a weekly basis. Our Service Providers may also acquire device identifiers and specific information about the browser you use. In some cases, this information may be unique to you.[44]

82. Nevertheless, in the June 13, 2023, Web Privacy Policy, Serviced Companies

[41] *Id*.
[42] Wythe Cnty. Cmty. Hosp., *Web Privacy Policy*, (as rev. June 13, 2023), https://www.wcch.org/privacy-policy, **Exhibit C.**
[43] *Id*.
[44] *Id*.

COPY

admitted that, for example, "'Protected health information' as defined under the Health Insurance Portability & Accountability Act and related regulations (collectively referred to as "HIPAA"), including information you provide to us while being treated as a patient or within the patient portal, **is separate and subject to our Notice of Privacy Practices**."[45]

83. Moreover, in Serviced Companies' Patient Rights and Responsibilities, Serviced Companies provided that patients have rights to, "[t]he privacy of [their] medical information and records, in accordance with state and federal law," and the right to "[p]ersonal privacy, private conversations."[46]

84. Despite these representations, HSCGP-managed Websites do indeed transfer Private Information to third parties. Using the Meta Pixel, HSCGP used and disclosed Plaintiffs' and Class Member's Private Information and confidential communications to Facebook, Google, and like other unauthorized third parties, without written authorization, and in violation of the Privacy Policies and Patient Rights and Responsibilities of Serviced Companies.

iv. HSCGP's Disclosure of Plaintiffs' and the Class Members' Private Information.

85. Defendant disclosed Plaintiffs' and Class Members' Private Information and confidential communications to Facebook and others by collecting and transmitting user interactions with HSCGP-managed Websites and sending records of those interactions to Facebook, via the Meta Pixel and other tracking technology, including, by way of example, those implemented: (i) on the Serviced Companies' home Websites page; (ii) on the "Find a Doctor" page; (iii) on the Serviced Companies' services page); (iv) on the pages for scheduling appointments; as well as (v) on the pre-portal page to login to the Patient Portal.

---

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

[46] Wythe Cnty. Cmty. Hosp., *Patient Rights and Responsibilities* (updated June 2023), https://www.wcch.org/sites/wythe/assets/uploads/New%20Folder/Patient%20Rights%20and%20Responsibilities.pdf.

COPY

86. For example, when a patient visits the Serviced Companies' Websites and clicks "Find a Doctor" the individual's browser sends a request to the Serviced Companies' server requesting that it load the webpage. Then, Meta Pixel sends secret instructions back to the individual's browser, causing it to imperceptibly record the patient's communication with the Serviced Companies and transmits it to Facebook's servers alongside personally identifying information, such as the patient's IP address. Thus, any Websites page a patient visits are then reported back to Facebook, alongside information identifying the patient.

87. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into its own massive datasets, before selling access to this data in the form of targeted advertisements. Employing "Audiences"—subsections of individuals identified as sharing common traits—Facebook promises the ability to "find the people most likely to respond to your ad."[47] Advertisers can purchase the ability to target their ads based on a variety of criteria: "Core Audiences," individuals who share a location, age, gender, and/or language;[48] "Custom Audiences," individuals who have taken a certain action, such as visiting a website, using an app, or buying a product bought a product;[49] and/or "Lookalike Audiences," groups of individuals who "resemble" a Custom Audience, and who, as Facebook promises, "are likely to be interested in your business because they're similar to your best existing customers.[50]

88. Google and other companies process data in a similar manner and use it to build marketing and other data profiles allowing for targeted advertising.

89. Defendant could have chosen not to use the Meta Pixel, or it could have configured

[47] Meta, *Audience Ad Targeting*, META ADS, https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 20, 2024).
[48] *Id.*
[49] *Id.*
[50] Meta Business Help Ctr., *How to Create a Lookalike Audience on Meta Ads Manager*, https://www.facebook.com/business/help/465262276878947 (last visited Nov. 20, 2024).

COPY

it to limit the information that it communicated to third parties, but it did not. Instead, it intentionally selected and took advantage of the features and functionality of the Pixel that resulted in the Disclosure of Plaintiffs' and Class Members' Private Information.

90. Along those same lines, Defendant could have chosen not to use Google and/or other tracking technologies to track Plaintiffs and Class Members private communications and transmit that information to unauthorized third parties. It did so anyway, intentionally taking advantage of these trackers despite the harm to Plaintiffs and Class Members' privacy.

91. Defendant used and disclosed Plaintiffs' and Class Members' Private Information to Facebook, Google, and possibly other third parties for the purpose of marketing its services and increasing its profits.

92. On information and belief, Defendant shared, traded, or sold Plaintiffs' and Class Members' Private Information with Facebook, and potentially other third parties, in exchange for improved targeting and marketing services.

93. Plaintiffs and the Class Members never consented, agreed, authorized, or otherwise permitted Defendant to intercept their communications or to use or disclose their Private Information for marketing purposes. They were never provided with any written notice that Defendant disclosed Protected Health Information to Facebook and others, nor were they provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Protected Health Information to unauthorized entities.

94. Plaintiffs and Class Members relied on Serviced Companies to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

95. Furthermore, Serviced Companies actively misrepresented that they would preserve

COPY

the security and privacy of Plaintiffs' and Class Members' Private Information. In actuality, Defendant shared data about Plaintiffs' and Class Members' activities on the Webpages alongside identifying details about the Plaintiffs and Class Members, such as their IP addresses.

96. By law, Plaintiffs and the Class Members are entitled to privacy in their Protected Health Information and confidential communications. Defendant deprived Plaintiffs and Class Members of their privacy rights when it (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiffs' and Class Members' confidential communications, Personally Identifiable Information, and Protected Health Information; (2) disclosed patients' Private Information to unauthorized, third-party eavesdroppers, including Facebook and possibly others; and (3) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent.

B. Plaintiffs' Experience

97. Plaintiffs are each patients of Serviced Companies, and received healthcare services from Serviced Companies and physicians in its network. They relied on Serviced Companies' Webpages to communicate confidential patient information.

98. Plaintiffs accessed Serviced Companies' Websites at ed Companies' direction and encouragement, including to find doctors including primary care doctors and gastrologist specialists to search for treatment services and provider information (e.g., via HSCGP-managed services page; and via the Patient Portal). They reasonably expected that their online communications with Serviced Companies, were confidential, solely between themselves and Serviced Companies and that, as such, those communications would not be transmitted to or intercepted by a third party.

99. Plaintiffs provided their Private Information to Serviced Companies and trusted that

COPY

the information would be safeguarded according to Serviced Companies' Privacy Policies and legal obligations.

100. As described herein, by use of the Meta Pixel and tracking technology, HSCGP sent Plaintiff's Private Information to Facebook and possibly others when Plaintiff used HSCGP-managed Websites to communicate healthcare and identifying information to Serviced Companies.

101. Pursuant to the process described herein, HSCGP assisted Facebook and possibly others with intercepting Plaintiff' confidential communications, including those that contained PII and PHI. HSCGP facilitated these interceptions without Plaintiffs' knowledge, consent, or express written authorization.

102. By failing to receive the requisite consent, HSCGP breached confidentiality and unlawfully disclosed Plaintiff' Private Information.

103. As a result of HSCGP's unauthorized Disclosure, Plaintiffs now receive targeted Facebook advertisements related to their personal health, when they did not provide Facebook with information related to their medical conditions or treatment.

C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI

104. In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[51] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

105. On February 18, 2021, the New York State Department of Financial Services

[51] Kurt Wagner & Bloomberg, *Facebook Admits Another Blunder with User Data*, FORTUNE (July 1, 2020, at 6:30 p.m.) https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/.

COPY

released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective . . . at preventing the receipt of sensitive data."[52]

106. The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[53] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[54]

107. More recently, Facebook employees admitted to lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "[w]e do not have an adequate level of control and explainability over how our systems use data,

[52] New York State Dep't of Fin. Servs., *Report on Investigation of Facebook Inc. Data Privacy Concerns*, (Feb. 18, 2021) https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf.
[53] Justin Sherman, *Your Health Data Might Be for Sale*, SLATE (June 22, 2022, at 5:50 a.m.) https://slate.com/technology/2022/06/health-data-brokers-privacy.html.
[54] *Id.*

COPY

and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'"[55]

108. Furthermore, in June 2022, an investigation by The Markup[56] revealed that the Meta Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.[57] On those hospital websites, the Meta Pixel collects and sends Facebook a "packet of data," including sensitive personal health information, whenever a user interacts with the website, for example, by clicking a button to schedule a doctor's appointment.[58] The data is connected to an IP address, which is "an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook."[59]

109. During its investigation, The Markup found that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[60]

110. In addition to the 33 hospitals identified by The Markup that had installed the Meta Pixel on their websites, The Markup identified seven health systems that had installed the Meta

---

[55] Lorenzo Franceschi-Bicchierai, *Facebook Doesn't Know What It Does with Your Data, or Where It Goes: Leaked Document*, VICE (April 26, 2022), https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.
[56] The Markup is a nonprofit newsroom that investigates how powerful institutions are using technology to change our society. *See* The Markup, *About Us*, www.themarkup.org/about (last accessed Nov. 20, 2024).
[57] Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022, 6:00 a.m.) https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.
[58] *Id.*
[59] *Id.*
[60] *Id.*

COPY

Pixel inside their password-protected patient portals.[61]

111. David Holtzman, health privacy consultant and former senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply troubled" by what the hospitals capturing and sharing patient data in this way.[62]

D. HSCGP Violated HIPAA Standards

112. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information (PHI) about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[63]

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

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

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[64]

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

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing

[61] *Id.*
[62] *Id.*
[63] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[64] U.S. Dep't of Health and Human Servs., *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, DHS.GOV (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

COPY

> purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).[65]

116. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technology.[66]

117. According to the Bulletin, "HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information."[67]

118. Citing The Markup's June 2022 article, the Bulletin expressly notes:

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

---

[65] U.S. Dep't of Health and Human Servs., *Marketing* (Dec. 3, 2002) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.
[66] *See* U.S. Dep't of Health and Human Servs., *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Nov. 20, 2024).
[67] *Id.*

COPY

> 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. [68]

119. In other words, HHS has expressly stated that Defendant's conduct of implementing the Meta Pixel on the Serviced Companies' websites is a violation of HIPAA Rules.

E. HSCGP Violated FTC Standards, and the FTC and HHS Take Action

120. The FTC has also recognized that implementation of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and "impermissibly disclos[e] consumers' sensitive personal health information to third parties."[69]

121. On July 20, 2023, the Federal Trade Commission (FTC) along with the U.S. Department of Health and Human Services (HHS) sent a "joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online activities."[70]

122. Therein, the FTC reminded healthcare providers of their HIPAA obligations: "HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA

---

[68] *Id.* (emphasis in original) (internal citations omitted).
[69] Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20, 2023) (available at https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), **attached as Exhibit A.**
[70] Fed. Trade Comm'n, *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies* (July 20, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery.

COPY

Rules."[71]

123. Additionally, the FTC reminded health providers of their "obligation to protect against impermissible disclosures of personal health information," adding that "[t]his is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes."[72]

124. Entities that are not covered by HIPAA also face accountability when consumers' sensitive health information is compromised under the FTC's Health Breach Notification Rule. 16 C.F.R. § 318. This requires that companies dealing with health records must notify the FTC and consumers if there has been a breach of unsecured identifiable health information, or else face civil penalties for violations. *Id*. According to the FTC, "a 'breach' is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, including sharing of covered information without an individual's authorization, triggers notification obligations under the Rule."[73]

125. The FTC Act makes it unlawful to employ "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" 15 U.S.C. § 45(a).

126. According to the FTC, "the disclosure of [sensitive health] information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a

[71] U.S. Dep't of Health & Human Services, *Re: Use of Online Tracking Technologies*, (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf, **Exhibit A.**
[72] *Id.*
[73] U.S. Fed. Trade Comm'n, *Statement of the Commission: On Breaches by Health Apps and Other Connected Devices* (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

COPY

breach of security under the FTC's Health Breach Notification Rule."[74]

127. In other words, the FTC and OCR have expressly stated that HSCGP's conduct of implementing the Facebook Pixel is a likely violation of the FTC Act and/or the FTC's Health Breach Notification Rule.

F. HSCGP Violated Industry Standards

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

129. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications, which are applicable to Serviced Companies and its physicians, and by association to their vendors such as HSCGP.

130. AMA Code of Ethics Opinion 3.1.1 provides:

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

131. AMA Code of Medical Ethics Opinion 3.2.4 provides:

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

---

[74] *See, e.g.*, *U.S. v. Easy Healthcare Corp.,* No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legallibrary/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In the Matter of BetterHelp, Inc.*, FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; *In the Matter of Flo Health Inc.,* FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/casesproceedings/192-3133-flo-health-inc.

COPY

132. AMA Code of Medical Ethics Opinion 3.3.2 provides:

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

G. Plaintiffs' and Class Members' Expectation of Privacy

133. At all times when Plaintiffs and Class Members provided their Private Information to Serviced Companies, they all had a reasonable expectation that the information would remain private and that Serviced Companies would not share the Private Information with third parties for a commercial marketing and sales purposes, unrelated to patient care.

H. IP Addresses are Personally Identifiable Information

134. Defendant also disclosed and otherwise assisted Facebook and potentially others with intercepting Plaintiffs' and Class Members' IP addresses using the Meta Pixel and other tracking technologies.

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

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

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

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

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

140. Under HIPAA, an IP address is Personally Identifiable Information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP

COPY

addresses. *See* 45 C.F.R. § 164.514 (2).

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

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

I. HSCGP Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

142. The sole purpose for Defendant's use of the Meta Pixel and other tracking technology was marketing and profits.

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

144. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients of Serviced Companies.

145. By utilizing the Meta Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting HSCGP and the Serviced Companies.

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

146. The data concerning Plaintiffs and Class Members, collected and shared by Defendant has tremendous economic value. Data collected via the Meta Pixel, CAPI, and other online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it then sells access in the form of targeted advertisements. Targeting works by allowing advertisers to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook,

COPY

are the "people most likely to respond to your ad."[75] Facebook's "Core Audiences" allow advertisers to target individuals based on demographics, such as age, location, gender, or language, whereas "Custom Audiences" allow advertisers to target individuals who have "already shown interest in your business," by visiting a business's website, using an app, or engaging in certain online content.[76] Facebook's "Lookalike Audiences" go further, targeting individuals who resemble current customer profiles and whom, according to Facebook, "are likely to be interested in your business."[77]

147. Data harvesting is big business, and it drives Facebook's profit center, its advertising sales. In 2019, Facebook generated nearly $70 billion dollars in advertising revenue alone, constituting more than 98% of its total revenue for that year.[78]

148. This business model is not limited to Facebook. Data harvesting one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

149. In particular, the value of health data is well-known due to the media's extensive reporting on the subject. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry." Therein, Time Magazine described the extensive market for health data and observed that the health data market is both

[75] Meta, *Audience Ad Targeting*, META Ads, https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 20, 2024).
[76] *Id.*
[77] *See* Meta Business Ctr., *How to Create a Lookalike Audience on Meta Ads Manager*, METAhttps://www.facebook.com/business/help/465262276878947 (last visited Nov. 20, 2024).
[78] *See* Rishi Iyengar, *Here's How Big Facebook's Ad Business Really Is*, CNN (July 1, 2020, at 9:19 at a.m.) https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html.

COPY

lucrative and a significant risk to privacy.[79]

150. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[80]

TOLLING, CONCEALMENT, AND ESTOPPEL

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

152. Defendant seamlessly incorporated Meta Pixel and other trackers into its Websites and Online Platforms while providing users with no indication that their Websites' usage was being tracked and transmitted to third parties. Defendant knew that the Websites it managed incorporated Meta Pixel and other trackers, yet it failed to disclose to Plaintiffs and Class Members that their sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook, and likely other third parties, including Google.

153. Plaintiffs and Class Members could not with due diligence have discovered the full scope of Defendant's conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel or any other tracking technology prior to June 13, 2023.

154. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Defendant's illegal interception and disclosure of Plaintiffs' and the Class Members' Private Information has continued unabated through the

[79] *See* Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, TIME, (Jan. 9, 2017, at 9:00 a.m.), https://time.com/4588104/medical-data-industry/.
[80] *See* Christina Farr, *Hospital Execs Say They are Getting Flooded with Requests for Your Health Data*, CNBC, (Dec. 18, 2019, at 8:27 a.m.), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

COPY

present. What's more, Defendant was under a duty to disclose the nature and significance of their data collection practices but did not do so. Defendant is therefore estopped from relying on any statute of limitations defenses.

CLASS ALLEGATIONS

155. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of other similarly situated persons.

156. The nationwide Class that Plaintiffs seeks to represent is defined as follows:

> all United States residents who, from August 1, 2021, to June 30, 2023, accessed the Patient Portal of any Serviced Company.

157. Excluded from the Settlement Class are (1) any Judge presiding over this Action, any members of the Judge's respective staffs, and immediate members of the Judge's family; (2) officers and directors of the Defendant, their subsidiaries, parent companies, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest; (3) persons who timely and validly request exclusion from and/or opt-out of the Settlement Class; and (4) the legal representatives, successors or assigns of any such excluded persons..

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

159. Numerosity: Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly used or disclosed by Defendant, and the Class is identifiable within Defendant and the Serviced Companies' records.

160. Commonality: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include

a. whether and to what extent Defendant had a duty to protect Plaintiffs' and Class

COPY

Members' Private Information;

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

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

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

e. whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' Private Information;

f. whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. whether Defendant failed to properly implement and configure the tracking software on its Online Platforms to prevent the disclosure of confidential communications and Private Information;

i. whether Defendant engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiffs' and Class Members' Private Information.

161. Typicality: Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's use and incorporation of Meta Pixel and other tracking technology.

162. Policies Generally Applicable to the Class: This class action is also appropriate for

COPY

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 policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendant 's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

163. 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 Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members 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.

164. 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 HSCGP. 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.

165. The nature of this action and the nature of laws available to Plaintiffs and Class

COPY

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. If the class action device were not used, Defendant would necessarily gain an unconscionable advantage because they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas 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. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

166. 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 demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

167. Adequate notice can be given to Class Members directly using information maintained in Defendant and the Serviced Companies' records.

168. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful use and disclosure and failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to and obtain proper consent from Class Member, and Defendant may continue to act unlawfully as set forth in this Complaint.

169. Further, Defendant has acted or refused to act on grounds generally applicable to the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

COPY

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

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

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

c. whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

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

e. whether Defendant breached the implied contract;

f. whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been used and disclosed to third parties;

g. whether Defendant failed to implement and maintain reasonable security procedures and practices;

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

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

COPY

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

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

172. Defendant owed to Plaintiffs and Class Members a duty to exercise reasonable care in handling and using Plaintiffs' and Class Members' Private Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Private Information that occurred.

173. Defendant acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiffs' and Class Members' Private Information by disclosing and providing access to this information to third parties for the financial benefit of the third parties and Defendant.

174. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's disclosure of their Private Information to benefit third parties and Defendant. Defendant actively sought and obtained Plaintiffs' and Class Members' Private Information.

175. Private Information is highly valuable, and Defendant knew, or should have known, the harm that would be inflicted on Plaintiffs and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and HSCGP by way of data harvesting, advertising, and increased sales.

176. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiffs and Class Members. This failure actually and

COPY

proximately caused Plaintiffs' and Class Members' injuries.

177. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, inappropriate advertisements, and use of their Private Information for advertising purposes, and increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

178. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs' and Class Members' actual, tangible, injury-in-fact and damages, including, without limitation, the unauthorized access of their Private Information by third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of use of their information that resulted from and were caused by Defendant's negligence. These injuries are ongoing, imminent, immediate, and continuing.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

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

180. Plaintiffs alleges this negligence *per se* theory as alternative to her other negligence claim.

181. Pursuant to the laws set forth herein, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, Defendant was required by

COPY

law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' Private Information.

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

183. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' PII and PHI, Private Information.

184. Defendant owed a duty to timely and adequately inform Plaintiffs and Class Members, in the event of their PII and PHI being improperly disclosed to unauthorized third parties.

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

186. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI and not complying with applicable industry standards as described in detail herein.

187. Defendant violated its duty as a Business Associate to Covered Entities under HIPAA and implementing regulations, the HIPAA Privacy Rule and Security Rule, by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI and not complying with applicable industry standards as described in detail herein.

188. Plaintiffs' and Class Member's PII and PHI constitute personal property that was taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury and

COPY

damages to Plaintiffs and Class Members.

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

190. In failing to secure Plaintiffs' and Class Members' PII and PHI, Defendant are guilty of oppression, fraud, or malice. Defendant acted or failed to act with a reckless, willful, or conscious disregard of Plaintiffs' and Class Members' rights. Plaintiffs, in addition to seeking actual damages, also seeks punitive damages on behalf of herself and the Class.

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

COUNT III
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On Behalf of Plaintiffs and the Class)

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

193. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Serviced Companies its Websites and the Patient Portals.

COPY

194. Plaintiffs and Class Members communicated sensitive PHI and PII—Private Information—that they intended for only Serviced Companies to receive and that they understood Serviced Companies would keep private.

195. 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 and their private affairs and concerns.

196. Plaintiffs and Class Members had a reasonable expectation of privacy given Serviced Companies' representations and conduct, including in its Privacy Policies and Patient Rights and Responsibilities, described above.

197. Moreover, Plaintiffs and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential. Defendant's disclosure of PHI coupled with PII is highly offensive to the reasonable person.

198. 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.

199. 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.

200. 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 because of its intrusions upon Plaintiffs' and Class Members' privacy.

201. 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

COPY

and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

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

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

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

204. As a condition of receiving medical care from Serviced Companies, Plaintiffs and the Class provided their Private Information and paid compensation for the treatment received. In so doing, Plaintiffs and Class Members entered into contracts with Serviced Companies by which Serviced Companies agreed to safeguard and protect such information, in its Privacy Policies and elsewhere, to keep such information secure and confidential, and to promptly and accurately notify Plaintiffs and the Class if their information had been breached and compromised or stolen.

205. Implicit in the agreement between Serviced Companies and its patients, Plaintiffs and the proposed Class Members, was the obligation that both parties would maintain the Private Information confidentially and securely.

206. Serviced Companies had an implied duty of good faith to ensure that the Private Information of Plaintiffs and Class Members in its possession was only used only as authorized, such as to provide medical treatment, billing, and other medical benefits from the Serviced Companies.

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

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

COPY

209. As manager of the Websites, Defendant also undertook these duties.

210. Plaintiffs and Class Members fully performed their obligations under the implied contract with Serviced Companies. Defendant acted in a manner contrary to Serviced Companies' obligations. Plaintiffs and Class Members would not have provided their confidential Private Information to Serviced Companies in the absence of their implied contracts with Serviced Companies and would have instead retained the opportunity to control their Private Information for uses other than receiving medical treatment from Serviced Companies.

211. Defendant breached the implied contracts with Plaintiffs and Class members by disclosing Plaintiffs' and Class Members' Private Information to an unauthorized third party.

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

213. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and the Class have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities.

214. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

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

216. This claim is pleaded solely in the alternative to Plaintiffs' breach of implied contract claim.

COPY

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

218. Plaintiffs and Class Members would not have used Defendant -managed Websites or would have paid less for those services, if they had known that HSCGP-managed Websites would collect, use, and disclose their Private Information to third parties.

219. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

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

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

222. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds it received as a result of its

COPY

conduct and the unauthorized Disclosure alleged herein.

COUNT VI
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

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

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

225. Defendant, in managing the Serviced Companies' websites, also undertook that fiduciary duty.

226. Defendant breached the fiduciary duty that it owed to Plaintiffs and the Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, and intentionally disclosing, their Private Information.

227. Defendant's breach of fiduciary duty was a legal cause of injury-in-fact and damage to Plaintiffs and the Class.

228. But for Defendant's breach of fiduciary duty, the injury-in-fact and damage to Plaintiffs and the Class would not have occurred.

229. Defendant's breach of fiduciary duty contributed substantially to producing the damage to the Plaintiffs and the Class.

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

COPY
EFILED 11/25/24 03:37 PM CASE NO. 23C2513 Joseph P. Day, Clerk

COUNT VII
VIOLATION OF TENN. CODE ANN. §§ 39-13-601, *et seq.*, AND SIMILAR STATE AND FEDERAL WIRETAP STATUTES
(On Behalf of Plaintiffs and the Class)

231. Plaintiffs re-alleges and incorporates the preceding paragraphs as if fully set forth herein.

232. Tenn. Code Ann. § 39-13-601 provides that a person commits an offense who:

> (A) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
> . . .
> (C) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection (a); or
>
> (D) Intentionally uses, or endeavors to use, the contents of any wire, oral or electronic communication, knowing or having reason to know, that the information was obtained through the interception of a wire, oral or electronic communication in violation of this subsection (a).

Tenn. Code Ann. § 39-13-601(a)(1).

233. For purposes of Tenn. Code Ann. § 39-13-601 "intercept" is "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device[.]" Tenn. Code Ann. § 40-6-303(11).

234. Defendant intentionally acquired and intercepted Plaintiffs' and Class Members' electronic communications without the consent of the Plaintiffs and Class Members, using the Meta Pixel and other trackers, in violation of Tenn. Code Ann. § 39-13-601.

235. Defendant intentionally acquired and intercepted Plaintiffs' and Class Members' electronic communications for the purpose of disclosing those communications to third parties, including Facebook, without the knowledge, consent, or written authorization of Plaintiffs or Class

COPY

Members, in violation of Tenn. Code Ann. § 39-13-601.

236. Defendant aided in the acquisition and interception of communications between Plaintiffs and Class Members and the Serviced Companies that were redirected and disclosed to and recorded by third parties without the Plaintiffs' or Class Members' consent.

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

a. those to which Plaintiffs' and Class Members' communications were disclosed;

b. Plaintiffs' and Class Members' personal computing devices;

c. Plaintiffs' and Class Members' web browsers;

d. Plaintiffs' and Class Members' browser-managed files;

e. the Meta Pixel;

f. internet cookies;

g. other pixels, trackers, and/or tracking technology installed on HSCGP-managed Websites and/or Patient Portals, including but not limited to Google trackers.

h. Serviced Companies' computer servers;

i. third-party source code utilized by HSCGP; and

j. computer servers of third parties (including Facebook).

238. Under Tenn. Code Ann. § 39-13-603, "any aggrieved person whose wire, oral or electronic communication is intentionally intercepted, disclosed, or used in violation of § 39-13-601 […] may in a civil action recover from the person or entity that engaged in that violation the following relief:

(1) The greater of:

COPY

> (A) The sum of the actual damages, including any damage to personal or business reputation or relationships, suffered by the Plaintiffs and any profits made by the violator as a result of the violation; or
>
> (B) Statutory damages of one hundred dollars ($100) a day for each day of violation or ten thousand dollars ($10,000), whichever is greater;
>
> (2) Punitive damages; and
>
> (3) A reasonable attorney's fee and other litigation costs reasonably incurred.

Tenn. Code Ann. § 39-13-603(a).

239. In addition to statutory damages, Defendant's violations of Tenn. Code Ann. § 39-13-601, caused Plaintiffs and Class Members the following damages:

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

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

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

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

e. Defendant's actions diminished the value of Plaintiffs' and Class Members' personal information.

240. Plaintiffs and the Class Members seek actual damages or statutory damages,

COPY

whichever is greater, arising from Defendant's violations of Tenn. Code Ann. § 39-13-601, punitive damages, as well as reasonable attorneys' fees and costs.

241. Defendant likewise violated the similar wiretap laws of the following states and are liable for statutory and or actual damages as a result: California (Cal. Penal Code § 637.2), Delaware (Del. Code tit. 11 §§ 2409, 2402), Florida (Fla. Stat. § 934.03), Illinois (720 Ill. Comp. Stat. 5/14-2, -6), Massachusetts (Mass. Laws ch. 272, § 99), Michigan (Mich. Comp. Laws Serv. § 750.539), Missouri (Mo. Ann. Stat. § 542.402, .418), Montana (Mont. Code Ann. §§ 45-8-208, 213), New Jersey (N.J. Stat. Ann. § 2A:156A), Nevada (Nev. Rev. Stat. § 200.620, 690), Ohio (Ohio Rev. Code Ann. §§ 2933.52, .65), Oregon (Or. Rev. Stat. Ann. §§ 165.540, 133.739), Pennsylvania (18 Pa. C.S. §§ 5704, 5725), Rhode Island (11 R.I. Gen. Laws Ann. §§ 11-35-21, 12-5.1-13), Texas (Tex. Civ. Prac. & Rem. Code Ann. §§ 123.001-.004), Utah (Utah Code Ann. § 77-23a), Virginia (Va. Code Ann. § 19.2-62, -64, -69), Washington (Wash. Rev. Code §§ 9.73.030, .060), and Wisconsin (Wis. Stat. Ann. § 968.31).

242. In addition, Defendant likewise violated the similar wiretap laws of the United States (18 U.S.C.A. § 2511

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, prays for judgment as follows:

A. for an Order certifying this action as a Class action and appointing Plaintiffs as Class Representative and Plaintiffs' counsel as Class Counsel;

B. for equitable relief enjoining HSCGP from engaging in the wrongful conduct

COPY

complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. for equitable relief compelling HSCGP to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Private Information compromised and unlawfully disclosed to third parties;

D. for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of HSCGP's' wrongful conduct;

E. an order HSCGP to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

F. an Order requiring HSCGP to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

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

H. for an award of punitive damages, as allowable by law;

I. for an award of attorneys' fees as permitted by the Tenn. CPA and Tenn. Code Ann. § 39-13-603;

J. costs and any other expenses, including expert witness fees incurred by Plaintiffs in connection with this action;

K. pre- and post-judgment interest on any amounts awarded; and

L. such other and further relief as this court may deem just and proper.

COPY
EFILED 11/25/24 03:37 PM CASE NO. 23C2513 Joseph P. Day, Clerk

DEMAND FOR JURY TRIAL

Dated: November 25, 2024

Respectfully submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV (#23045)
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Lynn A. Toops*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com

Samuel J. Strauss*
Raina Borelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
sam@straussborrelli.com
raina@straussborrelli.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
(866) 252-0878
gklinger@milberg.com

* *Pro Hac Vice admitted or admission forthcoming*

Counsel for Plaintiffs and the Proposed Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: HSCGP Settlement Resolves Class Action Lawsuit Over Alleged Data-Sharing Violations

---