ADAM B. WOLF (SBN 215914)
PEIFFER WOLF CARR KANE CONWAY & WISE LLP
awolf@peifferwolf.com
3435 Wilshire Blvd., Ste. 1400
Los Angeles, CA 90010
Telephone: (415) 766-3545
Facsimile: (415) 840-9435

[Additional counsel listed on signature page]

Attorneys for Plaintiff & the Proposed Class

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF CALIFORNIA

PATRICIA LEIJA, individually and on behalf of all others similarly situated, Plaintiff, v. **RITE AID CORPORATION**, a Delaware Corporation, Defendant.	CASE NO. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Patricia Leija ("Plaintiff"), on behalf of herself and all others similarly situated, by and through her attorneys of record, Peiffer Wolf Carr Kane Conway & Wise, LLP and Almeida Law Group LLC, brings this class action lawsuit against Rite Aid Corporation ("Rite Aid" or "Defendant"). The allegations set forth in this class action complaint are based on Plaintiff's personal knowledge, due investigation of undersigned counsel and—where indicated—upon information and good faith belief.

INTRODUCTION

1. Plaintiff brings this class action lawsuit to address Rite Aid's transmission and disclosure of Plaintiff's and Class Members' personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information") to Meta Platforms, Inc. d/b/a Meta ("Meta" or "Facebook") and other third parties via tracking

pixels ("Tracking Pixel" or "Pixel") and other tracking technologies installed on Defendant's website, www.riteaid.com (the "Website" or the "Digital Platforms").

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

3. During the Class Period, Rite Aid operated one of the largest chains of pharmacies in the United States, marketing, selling and profiting from its delivery of health care services and retail products to over one million Americans daily.[1] As of March 4, 2023, Defendant operated over 2,300 retail drugstores in seventeen states, with approximately one-third on the West Coast: 477 stores in California, 191 in Washington and 68 in Oregon.[2] Defendant also maintained and operated, and continues to maintain and operate, a website—https://www.riteaid.com—through which its customers can, among other things, learn about Defendant's services, find Rite Aid stores, fill their prescriptions, book various medical tests, schedule a number of different vaccinations and otherwise interact with Defendant.[3]

4. In the most recent reported year, fiscal 2023 (52 weeks ending March 4, 2023), over 71% of its total drugstore sales consisted of the sale of prescription drugs in its retail pharmacy segment, accounting for $12.6 billion. In that same reported year, one of the Rite Aid' s "key strategic drivers of growth" included "deepening [its] customer loyalty and engagement, by . . . leveraging personalized marketing and communications, and expanding [its] digital solutions."[4]

5. Rite Aid boasts about its technological advances and digital platforms without mentioning that it uses those platforms to—as a matter of course—disclose its customers' Private

[1] *See* Rite Aid Corporation, Fiscal 2023 Annual Report, Form 10-K, p. 5 (2023) (https://d18rn0p25nwr6d.cloudfront.net/CIK-0000084129/8c4c5776-a36e-498f-a981-f42c87b0975a.pdf).

[2] *Id.* at 45.

[3] Rite Aid Home Page, https://www.riteaid.com (last visited, July 18, 2023).

[4] Rite Aid Corporation, Fiscal 2023 Annual Report, Form 10-K, p. 8 (2023)

Information without obtaining their consent. For example, Rite Aid states in its most recent 10-K filing that:

> We launched our new website, mobile application, and ecommerce solution in fiscal 2021. This personalized user experience is built on a modern and scalable platform that will serve as the foundation for our digital and omnichannel solutions. **Looking ahead, we are focused on creating seamless digital pharmacy experiences that increase medication adherence and improve patient health, delivering signature customer experiences that delight customers and address traditional pharmacy pain points and providing easy digital onboarding capabilities for new pharmacy customer acquisition.** In addition to our digital work in pharmacy, we are also working to bring new and exciting omni-channel capabilities to market such as accelerating our buy-online pickup in store offerings, expanding our same day delivery partners and capabilities, and investing in best-in-class digital loyalty experiences.[5]

6. What Rite Aid has not publicly acknowledged is that customers would be unknowingly sacrificing their privacy by using Rite Aid's new website. When Plaintiff and other customers used Defendant's Website in order to refill a prescription, unbeknownst to Plaintiff and other customers, the names of their prescription medications, along with their personal information and personal identifiers, were secretly disclosed to Facebook, an unauthorized third party.

7. Through the Meta Pixel, a tracking tool intentionally incorporated by Rite Aid in its Website source code or otherwise affirmatively permitted on its website by Rite Aid, for customers who used the Manage Prescriptions feature of the Website to refill prescriptions, including Plaintiff, Defendant disclosed individually identifying information and information regarding their medical history, mental and physical condition, and treatment, to Facebook, all without its customers' knowledge and/or consent.

8. Thus, through its actions and practices, Rite Aid has disclosed Private Information to Facebook. This massive breach of confidentiality and privacy has, on information and belief,

[5] *Id*. at 9 (emphasis added).

affected millions of Rite Aid's customers in the state of California as well as millions more nationwide.

9. As detailed herein, Rite Aid's privacy policies provided no warning whatsoever that Class Members' PHI would be disclosed to Facebook for marketing purposes or otherwise. Rather, the applicable privacy policies stated that written authorization must be obtained from customers before their PHI is used or disclosed for marketing purposes.

10. Rite Aid never obtained such authorizations from Plaintiff or the Class Members.

11. Rite Aid's conduct violates its Patient Privacy Policy which promises that it will not share Users' Private Information for marketing purposes unless it first receives written authorization for that disclosure.[6]

12. Despite this representation—as well as many other similar ones in its privacy policy and elsewhere—that user data "is not shared without [] consent," through its actions, Rite Aid has acknowledged that it used invisible trackers by Facebook on its Digital Platforms. For example, in February 2023, Rite Aid was sued in a class action lawsuit for its use of the Meta Pixel to send Facebook highly sensitive PHI that Rite Aid collected from customers seeking to make a vaccine appointment.[7] Shortly after that lawsuit was filed, Rite Aid allegedly stopped sharing vaccine questionnaire information with Facebook—***but did not stop sharing its customers' personally identifiable prescription medication information with Facebook***. According to an article by The Markup:

> Rite Aid kept sharing prescription names even after the company stopped sharing answers to vaccination questions in response to the proposed class action (which did not mention the sharing of prescription information). Rite Aid did not respond to requests for comment, and as of June 23, the pixel was still present and sending

[6] *Rite Aid Corporation Notice of Privacy Practices*, https://www.riteaid.com/legal/patient-privacy-policy, RITEAID.COM (last visited July 19, 2023); *see also Rite Aid Corporation Privacy Policy*, https://www.riteaid.com/legal/privacy-policy, RITEAID.COM (last visited July 19, 2023).

[7] *See* Notice of Removal in *Doe et al. v. Rite Aid Corporation*, Case No. 3:23-CV-1495 (N.D. Cal. Mar. 29, 2023), p. 2 (describing the original case filed on Feb. 14, 2023).

the names of prescriptions to Facebook. [8, 9]

13. Despite the stigmas that unfortunately are so often associated with various medical issues and treatments, Rite Aid intentionally chose to put its profits over the privacy of its customers, which number several million.

14. The disclosure of Plaintiff's and Class Members' Private Information via the Pixel contravenes the letter and spirit of HIPAA's "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") which governs how health care providers must safeguard and protect Private Information. [10] The Privacy Rule is applicable to covered entities, which includes pharmacies that send PHI electronically, which includes all modern retail pharmacies such as Defendant.

15. The HIPAA Privacy Rule sets forth policies to protect all Individually Identifiable Health Information ("IIHI") that is held or transmitted by a covered entity such as Rite Aid. These are the 18 HIPAA Identifiers that are considered personally identifiable information because this information can be used to identify, contact, or locate a specific person or can be used with other sources (such as a person's Facebook account) to identify a single individual. When IIHI is used in conjunction with one's physical or mental health or condition, health care, and/or one's payment for that health care, it becomes PHI.[11]

---

[8] *Pixel Hunt: Need to Get Plan B or an HIV Test Online? Facebook May Know About It,* THEMARKUP.ORG, https://themarkup.org/pixel-hunt/2023/06/30/need-to-get-plan-b-or-an-hiv-test-online-facebook-may-know-about-it (last visited July 19, 2023).

[9] The lawsuit described in The Markup, *Doe et al. v. Rite Aid Corporation*, Case No. 3:23-CV-1495-AMO (N.D. Cal.), which was once amended, is presently pending before the Northern District of California, and makes no mention of prescription information being shared via the Meta Pixel or otherwise. As such, this instant suit is filed on behalf of a substantially different, and potentially much larger class, alleging conduct by Rite Aid that led to potentially millions of illegal disclosures for which no redress is presently being sought, prior to this filing.

[10] HHS.gov, The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited July 19, 2023).

[11] *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited July 19, 2023) (HIPAA Identifiers include name; address (all geographic

16. While healthcare entities regulated under HIPAA may use third-party tracking tools, such as Google Analytics or Meta Pixel, they can do so only in a very limited way, to perform analysis on data key to operations.

17. Simply put, further to the HIPAA Privacy Rule, covered entities such as Defendant are simply ***not*** permitted to use tracking technology tools (like pixels) in a way that exposes patients' Private Information to any third party without express and informed consent.

18. Lest there be any doubt of the illegal nature of Defendant's practice, the Office for Civil Rights (OCR) at HHS has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the unlawful transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[12]

19. Moreover, Rite Aid breached its statutory and common law obligations to Plaintiff and Class Members by, *inter alia*,: (i) failing to adequately review its marketing programs and web based technology to ensure its Digital Platforms were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class

---

subdivisions smaller than state, including street address, city county, and zip code); all elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age); telephone numbers; email address; medical record number; health plan beneficiary number; account number; device identifiers and serial numbers; web URL; internet protocol (IP) address; and any other characteristic that could uniquely identify the individual).

[12] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html, HHS.GOV (emphasis added) (last visited July 19, 2023).

Members' Private Information through Pixels; (v) failing to warn Plaintiff and Class Members that their Private Information was being shared with third parties without express consent; and (vi) otherwise failing to design, and monitor its Digital Platforms to maintain the confidentiality and integrity of patient Private Information.

20. Rite Aid's actions constitute an extreme invasion of Plaintiff's and Class Members' privacy. Rite Aid's actions also violated common law, the California Constitution, and numerous federal and state statutes.

21. As a result, Plaintiff and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) diminution of value of the Private Information; (iv) statutory damages and (v) the continued and ongoing risk to their Private Information.

22. Plaintiff brings this class action on behalf of herself and all natural persons residing in California who used Defendant's website to refill a prescription and whose PHI was disclosed or transmitted to Meta or any other unauthorized third party (hereinafter, "California Class Members").

23. Plaintiff also brings this class action on behalf of herself and all natural persons who used Defendant's website to refill a prescription and whose PHI was disclosed or transmitted to Meta or any other unauthorized third party (hereinafter, "Nationwide Class Members" and, collectively with California Class Members, hereinafter "Class Members").

PARTIES

24. Plaintiff Patricia Leija is a citizen of California residing in Hanford, Kings County, California. Plaintiff used Defendant's website to refill a prescription in or about October 2022. As a result, her PHI was disclosed to Meta without her knowledge, consent or authorization.

25. Defendant Rite Aid Corporation, is a Delaware Corporation. Rite Aid's principal place of business, as listed with the California Secretary of State, is 30 Hunter Lane in Camp Hill, Pennsylvania 17011. On information and belief, Rite Aid has moved its corporate headquarters and principal place of business to 1200 Intrepid Avenue, 2nd Floor in Philadelphia, Pennsylvania 19112. Rite Aid is licensed to do business in the state of California.

JURISDICTION & VENUE

26. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs, and minimal diversity exists because at least one class member and Defendant are citizens of different states.

27. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint alleges violation of federal laws, including the Electronic Communications Privacy Act ("ECPA"), 28 U.S.C. § 2511, *et seq*.

28. The Court has personal jurisdiction over Rite Aid because it regularly engages in extensive business throughout the country and the State of California, including through its hundreds of drugstores in California.

29. Venue is proper in this District pursuant to 28 U.S.C.§ 1391(b)(1) because many of the acts and/or omissions giving rise to the claims asserted herein occurred in this judicial district.

FACTUAL BACKGROUND

A. In Order for Plaintiff & Class Members to Fill Prescriptions on its Website, Defendant Required Their PHI to Be Stored on its Website

30. Throughout the Class Period, Defendant maintained and operated websites (including www.riteaid.com), by and through which Defendant encouraged and permitted consumers to refill medications for millions of prescriptions.

31. To refill a prescription, Class Members were first required to set up their online patient portal account with Rite Aid, which required the Class Member to provide their first name; last name; street address; city; state; zip code; and other personally identifying information. Based on this information, the Class Member's prescriptions previously filled or transferred to Rite Aid were linked to the Class Member's Rite Aid account.

32. To begin the process of refilling a prescription, when a Class Member visited Defendant's website they could, from the home page, after signing into their account, click on the "Refill Your Rx" button. Having clicked on that button, the Class Member would be taken to a page with the heading "Choose from prescription history," and would be required to select one or more

prescription medications to refill, and to click "Continue."

33. On information and belief, throughout the Class Period, the process for refilling a prescription on Defendant's website has been substantially the same in all material respects throughout the United States.

34. Thus, in order to use Defendant's website to refill a prescription, Plaintiff and other Class Members were required by Defendant's website to store confidential, private, and sensitive personal and health information on its website servers, and to have that information stored along with their personal identifiers.

B. Defendant Secretly Disclosed, & Permitted Meta to Intercept, Plaintiff's & Class Members' PHI.

35. Completely unbeknownst to Plaintiff and other Class Members, and continuing to the present, PHI that they communicated to Defendant through Defendant's website while refilling a prescription was intercepted by and/or disclosed to at least one unauthorized third party: Meta.

Defendant's Pixel, Source Code & Interception of HTTP Requests

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

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

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

> **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.

- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.

- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data. [13]

39. A patient's HTTP Request essentially asks Rite Aid's Website to retrieve certain information (such as a customer's prescribed medication name), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the customer's screen as they navigate Defendant's Website).

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

41. 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. The Pixel and other tracking technologies Rite Aid uses constitute source code that does just that. These tracking technologies thus act much like a traditional wiretap.

42. Rite Aid encourages customers to use its Digital Platforms to refill prescriptions and take other actions related to their personal health care. When interacting with Rite Aid's Digital Platforms like this, Plaintiffs and Class Members convey highly private and sensitive information to Rite Aid.

43. When patients visit Rite Aid's Digital Platforms via an HTTP Request to Rite Aid's server, that server sends an HTTP Response including the Markup that displays the webpage visible to the user and Source Code, including Rite Aid's Pixel.

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

44. Thus, Rite Aid is in essence handing patients a tapped device, and once the webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Website to trigger the tap, which intercepts those communications intended only for Rite Aid and transmits those communications to third parties, including Facebook, Google, TikTok, and others.

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

46. Defendant intentionally configured Pixels installed on its Website to capture both the "characteristics" of individual patients' communications with the Defendant's Websites (e.g., their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (i.e., the buttons, links, pages, and tabs they click and view, as well as search terms entered into free text boxes and descriptive URLs showing the information being exchanged).

47. Defendant also deposits cookies named _fbp, _ga_, and _gid onto Plaintiff's and Class Members' computing devices. These are cookies associated with the third-parties Facebook and Google but which Defendant deposits on Plaintiff's and Class Members' computing devices by disguising them as first-party cookies. Without any action or authorization, Defendant commands Plaintiff's and Class Members' computing devices to contemporaneously re-direct the Plaintiff's and Class Members' identifiers and the content of their communications to Facebook and Google.

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

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

50. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that cannot be evaded by savvy users. Facebook's workaround, for example, is called Conversions API (CAPI).

51. CAPI is an effective workaround because it does not intercept data communicated from the user's browser. Instead, Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."

52. Thus, as to Conversions API, the communications between patients and Rite Aid, which are necessary to use its Website, are actually received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those communications directly from Rite Aid to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

53. While there is no way to confirm with certainty that a Web host like Rite Aid has implemented workarounds like Conversions API without access to the host server, companies like Facebook instruct Rite Aid to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[14]

54. Thus, it is reasonable to infer that Facebook's customers who implement its Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround.

55. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user's communications. Instead,

---

[14] *See Best Practices for Conversions API,* https://www.facebook.com/business/help/308855623839366?id=818859032317965, FACEBOOK.COM (last visited March 21, 2023).

these third parties are typically procured to track user data and intercept their communications for the marketing purposes of the website owner.

56. Thus, without any knowledge, authorization, or action by a user, a website owner like Rite Aid can use its source code to commandeer a user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

57. In this case, Rite Aid employed just such devices (the Tracking Pixel, Google Tag Manager, and similar technologies) to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to third parties like Facebook and Google.

58. The Pixel, a marketing product, is a "piece of code" that allowed Defendant to "understand the effectiveness of [their] advertising and the actions [patients] take on [their] site."[15] It also allowed Defendant to optimize the delivery of ads, measure cross-device conversions, create custom advertising groups or "audiences," learn about the use of its Website, and decrease advertising and marketing costs.[16]

59. Most importantly, it allowed Facebook to secretly intercept customers' communications about their medical prescriptions on Defendant's Website.

Facebook's Platform & its Business Tools

60. 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.[17]

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

---

[15] https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited June 7, 2023).

[16] *Id.*

[17] META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx, INVESTOR.FB.COM (last visited June 7, 2023).

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

63. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[18]

64. Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[19]

65. One such Business Tool is the Pixel which "tracks the people and type of actions they take."[20]

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

67. This second, contemporaneous, and secret transmission contains the original GET request sent to the host website, along with additional data that the Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the

---

[18] *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142, FACEBOOK.COM (last visited June 7, 2023); *see*, META PIXEL, GUIDES, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/, FACEBOOK.COM (last visited June 7, 2023); *see also* BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142, FACEBOOK.COM (last visited June 7, 2023); META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/, FACEBOOK. COM (last visited June 7, 2023).

[19] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142, FACEBOOK.COM (last visited June 7, 2023); *see also* META MARKETING API, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[20] RETARGETING, https://www.facebook.com/business/goals/retargeting, FACEBOOK. COM (last visited June 7, 2023).

host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's Website—Defendant's own code, and Facebook's embedded code.

68. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients' Facebook IDs, IP addresses, and/or device IDs and the other information they input into Defendant's Website, including not only their medical searches, treatment requests, and the webpages they view, but also their name, email address, or phone number. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[21] Plaintiff's and Class Members identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

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

70. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

71. This disclosed PHI and PII allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought (in the case of Rite Aid, obtaining prescription medications), and the third party then sells that information to marketers who will online target Plaintiffs and Class Members.

[21] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited June 7, 2023).

C. ***Defendant Disclosed Plaintiff's & Class Members' PHI to Meta & Used Plaintiff's & Class Members' PHI for its Own Purposes***

72. Starting on date unknown and continuing to the present, Defendant embedded the Meta Pixel on and throughout its website and transmitted PHI shared by Plaintiff and Class Members, without their consent, to Meta in accordance with the Meta Pixel's configuration.

73. Rite Aid installed the Meta Pixel on its website - www.riteaid.com. When Plaintiff or another Class Member visited that website and completed the steps necessary to refill a prescription, the Meta Pixel automatically caused the Plaintiff's or Class Member's personal identifiers, including IP addresses and the c_user, _fr, _datr, and _fbp cookies, to be transmitted to Meta, attached to the fact that the Plaintiff or Class Member had visited the website and the titles of the webpages the Plaintiff or Class Member visited.

74. Rather than merely transmit the "automatic events" that the Meta Pixel automatically collects and transmits from a website without the website owner or developer being required to add any additional code, on information and belief, Defendant intentionally configured the Meta Pixel on its website to track, collect, and disclose "custom events" such as the name of the prescription medication that a customer was seeking to refill.

75. Moreover, the Meta Pixel on Defendant's website was also intentionally configured or authorized to use a feature called "automatic advanced matching." That feature scans forms on a website looking for fields that may contain personally identifiable information like a first name, last name, or email address, and then causes that information to be disclosed to Meta. On Defendant's website this feature collected, at a minimum, the first names and last names of Plaintiff and other Class Members as displayed on the Prescription Management page of the Website.

76. The data collected by the automatic advanced matching feature is disclosed to Meta in an obfuscated form know as a "hash." But Meta is able to determine the pre-obfuscated version of the data. Indeed, Meta uses the hashed information to link other data collected and disclosed by the Meta Pixel to Plaintiff's and Class Members' Facebook and Instagram profiles.

77. Thus, put simply, when Plaintiff or other Class Members used Defendant's website to refill a prescription, their identities, personal identifiers, and health information (together their

PHI) was disclosed to Meta.

78. On information and belief, Defendant disclosed Plaintiff's and Class Members' PHI to Meta in order to permit Defendant to improve its marketing and advertising, in order to increase Defendant's revenues and profits. Thus, Defendant used Plaintiff's and Class Members' PHI for its own marketing and advertising purposes, in an attempt to increase its own revenues and profits.

D. Rite Aid Does Not Disclose That It Sends Private Information to Third Parties for Marketing Purposes & Violates Its Own Privacy Policies

79. Rite Aid's privacy policies represent to Plaintiff and Class Members that it will keep Private Information private and secure and that it will only disclose Private Information under certain circumstances, ***none of which is true***.

80. These Privacy Policies state that Plaintiffs' and Class Members' Private information will not be shared for marketing purposes without prior, written permission.

81. Plaintiffs and Class Members have not provided Rite Aid with written permission to share their Private Information for marketing purposes.

82. Specifically, Rite Aid publishes a Notice of Privacy Practices which tells patients that "in accordance with the Health Insurance Portability and Accountability Act of 1996 ('HIPAA') Privacy Rule," Rite Aid "may use and disclose [customers'] protected health information [PHI] to carry out treatment, payment or health care operations ***and for other specific purposes that are permitted or required by law***."

83. The Notice of Privacy Practices sets out certain limited uses of protected health information for the purposes of "Treatment, Payment and Health Care Operations." It states: "We will use your [PHI] to treat you," We will use your [PHI] to obtain payment for products and services," and "We will use your [PHI] to carry out health care operations." After each of these statements, the Notice of Privacy Practices provides additional detail about how a customer's PHI might be used for each respective purpose.

84. The Notice of Privacy Practices then sets out "uses and disclosures that are either permitted or required by the HIPAA Privacy Rule." The Notice explains: "Using their professional judgment, our pharmacists may disclose your protected health information to a family member,

other relative, close personal friend, or any person you identify as being involved in your health care. This could include allowing those persons to pick up filled prescriptions, medical supplies, or medical records on your behalf. We may enter into contracts with some entities known as Business Associates that perform services for us. For example, we sometimes engage Business Associates to sort insurance or other third party payor claims for submission to the actual payor. We may disclose protected health information to our Business Associates so that they can perform their services and then bill your third party payor for services rendered. We require the Business Associates to appropriately safeguard the protected health information."

85. Next, the Notice of Privacy Practices details "other required or permitted disclosures of [PHI]." The Notice contains an exhaustive list of these other potential disclosures, including, for example: "to law enforcement agencies as required by law or in response to a valid subpoena or other legal process," "to a coroner or medical examiner when necessary, for example, to identify a deceased person or to determine a cause of death, or to funeral directors consistent with applicable law to carry out their duties," "when necessary to prevent a serious threat to the patient's health and safety or the health and safety of the public or another person," and "to authorized federal officials so they may provide protection to the President, other authorized persons, or foreign heads of state or conduct special investigations."

86. Rite Aid's privacy policy does ***not*** permit it to use and disclose Plaintiff's and Class Members' Private Information for marketing purposes. Rather, the Notice of Privacy Practices provides: "***We will obtain your written Authorization before using or disclosing protected health information about you for marketing purposes, to sell your protected health information***, or for purposes other than those listed above or otherwise permitted or required by law. You may revoke an Authorization in writing at any time. Such revocations must be made in writing. Upon receipt of the written revocation, we will stop using or disclosing protected health information about you, except to the extent that we have already taken action in reliance on the Authorization." (emphasis added).

87. Plaintiff's and Class Members' PHI, as that term is defined in this Complaint, is "protected health information" within the meaning of HIPAA and, thus, Defendant's Notice of Privacy Practices.

88. Rite Aid's promise that it will not sell its users' Private Information without their authorization and consent is false.

89. Rite Aid violated its own privacy policies by unlawfully intercepting and disclosing Plaintiffs' and Class Members' Private Information to Facebook and other third parties without acquiring Plaintiffs' and Class Members' consent or authorization to share the Private Information.

90. Even non-Facebook users can be individually identified via the information gathered on the Digital Platforms, like an IP address or personal device identifying information. This is precisely the type of information for which HIPAA requires the use of de-identification techniques to protect patient privacy.[22]

91. In fact, in an action pending against Facebook related to use of its pixel on healthcare provider web properties, Facebook explicitly stated it requires Pixel users to "post a prominent notice on every page where the pixel is embedded and to link from that notice to information about exactly how the pixel works and what is being collected through it, so it is not invisible."[23]

92. Defendant not only did not post such a notice, but it falsely represented it would notify affected victims should a breach of unsecured PHI take place.

93. Facebook further stated that "most providers [...] will not be sending [patient information] to Meta because it violates Meta's contracts for them to be doing that."[24]

---

[22] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited June 4, 2023).

[23] *See* Transcript of the argument on Plaintiff's Motion for Preliminary Injunction in *In re Meta Pixel Healthcare Litigation*, Case No. CV-22-03580-WHO (N.D. Cal. Nov. 9, 2022) (Hon. J. Orrick), at 19:12-18; *see also In re Meta Pixel Healthcare Litig.*, 2022 WL 17869218 (N.D. Cal. Dec 22, 2022).

[24] *Id.*, *supra* note 16, at 7:20-8:11.

94. Despite a lack of disclosure, Rite Aid allowed third parties to "listen in" on patients' confidential communications and to intercept and use for advertising purposes the very information it promised to keep private, in order to bolster its profits.

E. Rite Aid's Use of the Pixel Violates HIPAA

95. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[25]

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

97. The Privacy Rule broadly defines PHI as IIHI that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

98. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

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

A. Names;

---

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

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

45 C.F.R. § 160.514.

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

101. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be Protected Health Information. The Department of Health and Human Services has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data, "[i]f such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI."[26]

[26] *See Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, HHS.GOV (last visited June 4, 2023).

102. Consistent with this restriction, the HHS has issued marketing guidance that provides, "With limited exceptions, the [Privacy] Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list."[27]

103. Here, Defendant provided patient information to third parties in violation of the Privacy Rule.

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

105. Rite Aid further failed to comply with other HIPAA safeguard regulations as follows:

a. Failing to ensure the confidentiality and integrity of electronic PHI that Rite Aid created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1);

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

c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Rite Aid in violation of 45 C.F.R. § 164.308(a)(6)(ii);

[27] *Marketing*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html, HHS.GOV (last visited June 7, 2023).

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

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

f. Failing to ensure compliance with HIPAA security standard rules requiring adequate workforce comprehensive training instead of training software used to test staff by imitating phishing emails in violation of 45 C.F.R. § 164.306(a)(4);

g. Failing to effectively train its workforce (including independent contractors) on the policies and procedures for PHI as necessary and appropriate to carry out job functions while maintaining security of PHI beyond using imitation phishing email software in violation of 45 C.F.R. §§ 164.530(b) and 164.308(a)(5); and

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

106. 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 instructed in 2012:

> 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.[28]

107. In its guidance for Marketing, the Department further instructed in 2003:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added).[29]

108. HHS has repeatedly instructed for years that patient status is protected by the HIPAA Privacy Rule:

a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002); and

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013).

109. 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

---

[28] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* (Nov. 26, 2012) at 5, available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022).

[29] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (April 3, 2003) (last visited Nov. 3, 2022).

Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[30]

110. The Bulletin expressly provides that "**[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.**"[31]

111. Tracking technology vendors like Facebook and Google are considered business associates under HIPAA where, as here, they provide services to Defendant and receive and maintain PHI.

> Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (*e.g.* health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.[32]

112. The Bulletin further explained that health care providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address) even if no treatment information is included and even if the individual does not have a relationship with the health care provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?

---

[30] *See* HHS.gov, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited May 5, 2022).

[31] *Id.* (emphasis in original).

[32] *Id.*

> Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually identifiable health information (IIHI) that the individual providers when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. **This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e. it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care**.[33]

113. HIPAA applies to Defendant's webpages with tracking technologies even outside the patient portal:

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

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

apply.[34]

114. HHS also explained in the Bulletin that tracking technologies on health care providers' patient portals "generally have access to PHI" and may access diagnoses and treatment information, in addition to other sensitive data:

> Tracking on user-authenticated webpages
>
> Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. **Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to only use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.[35]

115. The Bulletin is not a pronouncement of new law, but instead reminded covered entities and business associates of their longstanding obligations under existing guidance. The Bulletin notes that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," then explains how online tracking technologies violate the same HIPAA rules that have existed for decades.[36]

---

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

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

[36] *Id.* (citing, *e.g.*, Modifications of the HIPAA [Rules], Final Rule," 78 FR 5566, 5598, a rulemaking notice from January 25, 2013, which stated: "[P]rotected health information … may not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a covered entity, then

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

F. Rite Aid Violated Industry Standards.

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

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

119. 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)[.]

120. 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.

121. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must: (c) Release patient information only in keeping ethics guidelines for confidentiality.[37]

---

it is protected health information by definition since it is indicative that the individual received health care services or benefits from the covered entity, and therefore it must be protected … in accordance with the HIPAA rules.").

[37] AMA Principles of Medical Ethics: I, IV, *Chapter 3: Opinions on Privacy, Confidentiality & Medical Records*, https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf, American Medical Association (last visited Mar. 21, 2023).

122. Rite Aid's use of the Pixel also violates Federal Trade Commission ("FTC") data security guidelines. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

123. The FTC's October 2016 publication *Protecting Personal Information: A Guide for Business*[38] established cyber-security guidelines for businesses.

124. These guidelines state that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network vulnerabilities; and implement policies to correct any security problems.

125. Upon information and good faith belief, Rite Aid failed to implement these basic, industry-wide data security practices.

G. Users' Reasonable Expectation of Privacy.

126. Plaintiff and Class Members were aware of Rite Aid's duty of confidentiality when they sought medical services from Rite Aid.

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

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

129. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing

[38] Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jun. 2, 2023).

consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[39]

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

H. IP Addresses are Protected Health Information.

131. Based on information and belief, Rite Aid improperly disclosed Plaintiff's and Class Members' computer IP addresses to third parties like Facebook and Google through its use of the Pixel *in addition to* names, phone numbers, email addresses, dates of birth, Rite Aid client ID numbers, services selected, assessment responses, patient statuses, medical conditions, treatments, provider information, and appointment information.

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

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

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

135. Facebook tracks every IP address ever associated with a Facebook user. Google also tracks IP addresses associated with Internet users.

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

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

[39] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/, CONSUMERREPORTS.ORG (last visited Jun. 2, 2023).

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

139. Consequently, Rite Aid's disclosure of Plaintiff's and Class Members' IP addresses violated HIPAA and industry-wide privacy standards.

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

140. The primary motivation and a determining factor in Defendant's interception and disclosure of Plaintiff's and Class Members' Private Information was to commit criminal and tortious acts in violation of federal and state laws as alleged herein, namely, the use of patient data for advertising in the absence of express written consent. Defendant's further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was in violation of HIPAA and an invasion of privacy. In exchange for disclosing the personally identifiable information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on Facebook

141. Rite Aid used the Pixel on its Digital Platforms for its own purposes of marketing and profits.

142. Based on information and belief, Rite Aid receives compensation from third parties like Facebook and Google in the form of enhanced advertising services and more cost-efficient marketing on third-party platforms in exchange for disclosing patients' personally identifiable information.

143. Based on information and belief, Rite Aid was advertising its services on Facebook, for one, and the Pixel was used to "help [Defendant] understand which types of ads and platforms are getting the most engagement[.]"[40]

[40] RETARGETING, https://www.facebook.com/business/goals/retargeting, FACEBOOK. COM (last visited June 5, 2023).

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

145. Upon information and belief, Rite Aid re-targeted patients and potential patients to get more people to use its services. These patients include Plaintiff and Class Members.

146. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting and enriching Rite Aid.

J. Class Members' Data Had Financial Value

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

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

149. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[41]

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."[42]

151. Several companies have products through which they pay consumers for a license to track certain information. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing history information.

152. Facebook itself has paid users for their digital information, including browsing history. Until 2019, Facebook ran a "Facebook Research" app through which it paid $20 a month

---

[41] *See* https://time.com/4588104/medical-data-industry/ (last visited June 7, 2023).

[42] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited June 7, 2023).

for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

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

154. Policymakers are proactively calling for a revision and potential upgrade of the HIPAA privacy rules out of concern for what might happen as tech companies continue to march into the medical sector.[43]

155. Private Information is also a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use Private Information to commit an array of crimes that include identity theft and medical and financial fraud.[44] A robust "cyber black market" exists where criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

156. While credit card information and associated IIHI can sell for as little as $1–$2 on the black market, PHI can sell for as much as $363.[45]

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

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

---

[43] *Id.*

[44] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Mar. 16, 2023).

[45] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed Mar. 16, 2023).

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

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

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

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

162. Rite Aid gave away Plaintiffs' and Class Members' communications and transactions on its Digital Platforms without permission.

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

K. Defendant Used and Disclosed Plaintiff's & Class Members' PHI Without Plaintiff's or Class Members' Knowledge, Consent, Authorization or Further Action

164. The tracking tools incorporated into, embedded in, or otherwise permitted on Defendant's website were invisible to Plaintiff and Class Members while using that website. The Meta Pixels on Defendant's website were seamlessly integrated into the website such that there was no reason for Plaintiff or any Class Member to be aware of or to discover their presence.

165. Plaintiff and Class Members were shown no disclaimer or warning that their PHI would be disclosed to any unauthorized third party without their express consent.

166. Plaintiff and Class Members had no idea that their PHI was being collected and transmitted to an unauthorized third party.

167. Because Plaintiff and Class Members had no idea of the presence of Meta Pixels on

Defendant's website, or that their PHI would be collected and transmitted to Meta, they could not and did not consent to Rite Aid's conduct.

168. Plaintiff and Class Members did not give consent or authorization for Defendant to disclose their PHI to Meta or to any third party for marketing purposes.

169. Moreover, Defendant's Notice of Privacy Practices, as described above, provided no indication to Plaintiff or Class Members that their PHI would be disclosed to Meta or any unauthorized third party.

TOLLING, CONCEALMENT & ESTOPPEL

170. Any applicable statutes of limitation have been tolled by Defendant's knowing and active concealment of its incorporation of the Meta Pixel into its website.

171. The Meta Pixel and other tracking tools on Defendant's website were and are entirely invisible to a website visitor.

172. Through no fault or lack of diligence, Plaintiff and Class Members were deceived and could not reasonably discover Defendant's deception and unlawful conduct.

173. Plaintiff was ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their part.

174. Defendant had exclusive knowledge that its website incorporated the Meta Pixel and other tracking tools and yet failed to disclose to customers, including Plaintiff and Class Members, that by refilling prescriptions through Defendant's website Plaintiff's and Class Members' PHI would be disclosed or released to Meta.

175. Under the circumstances, Defendant was under a duty to disclose the nature, significance, and consequences of its collection and treatment of its customers' PHI. In fact, to the present Defendant has not conceded, acknowledged, or otherwise indicated to its customers that it has disclosed or released their PHI to unauthorized third parties. Accordingly, Defendant is estopped from relying on any statute of limitations.

176. Moreover, all applicable statutes of limitation have also been tolled pursuant to the discovery rule.

177. The earliest that Plaintiff or Class Members, acting with due diligence, could have reasonably discovered Defendant's conduct would have been shortly before the filing of this Complaint.

ALLEGATIONS SPECIFIC TO PLAINTIFF

178. In or about October 2022, and numerous other times, Plaintiff Patricia Leija visited Rite Aid's website, while in California, and sought to refill a prescription.

179. By interacting with the Prescription Management function on Defendant's Digital Platforms, Plaintiff's PHI was disclosed to Meta, including, but not limited to, the names of her prescription medications.

180. Plaintiff would not have used Rite Aid's website to refill a prescription had she known that her PHI would be disclosed to unauthorized third parties.

181. Plaintiff believed that because she was on the website of a healthcare provider and pharmacy, her PHI would be protected and kept confidential.

182. Plaintiff saw nothing on Defendant's website that suggested to her that her PHI would be disclosed or released to an unauthorized third party.

183. Plaintiff did not authorize, consent to, or otherwise engage or permit the release of their PHI to Meta or any third party.

CLASS ACTION ALLEGATIONS

184. Plaintiff brings this action, on behalf of herself and all others similarly situated, as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure. Plaintiff seeks to represent two Classes, defined as follows:

The California Class

"All natural persons residing in California who used Defendant's Website to refill a prescription and whose PHI was disclosed or transmitted to Meta or any other unauthorized third party."

The Nationwide Class

"All natural persons who used Defendant's Website to refill a prescription and whose PHI was disclosed or transmitted to Meta or any other unauthorized third party."

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

186. Plaintiff reserves the right to modify or to amend the definition of the proposed classes before the Court determines whether certification is appropriate.

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

188. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to each Class exist and predominate over any questions affecting only individual Class Members. These include:

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

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

c. Whether Defendant violated its Privacy Policies by disclosing the Private Information of Plaintiff and Class Members to Facebook and/or additional third parties;

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

e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

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

g. Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

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

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

j. Whether Defendant knowingly made false representations as to its data security and/or Privacy Policy practices;

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

l. Whether Defendant's knowing disclosure of its patients' individually identifiable health information to Facebook is "criminal or tortious" under 18 U.S.C § 2511(2)(d); and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm they face as a result of Defendant's disclosure of their Private Information.

189. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's use of Pixels, due to Defendant's misfeasance.

190. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

191. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims

in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

192. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's 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.

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

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

195. Based on information and belief, adequate and direct notice can be given to Class Members using information maintained in Defendant's records.

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

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

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

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

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

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

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

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

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

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

CALIFORNIA LAW SHOULD APPLY TO PLAINTIFF'S & CLASS MEMBERS' COMMON LAW CLAIMS

199. The State of California has a significant interest in regulating the conduct of businesses operating within its borders.

200. California, which seeks to protect the rights and interests of California and all residents and citizens of the United States against a company operating 477 retail pharmacies in California—far more than any other state, has a greater interest in the claims of Plaintiffs and the Classes than any other state and is most intimately concerned with the claims and outcome of this litigation.

201. Defendant's breaches of duty to Plaintiff and a substantial portion of the Class Members emanated from California.

202. Application of California law to the Classes with respect to Plaintiff's and the Classes' common law claims is neither arbitrary nor fundamentally unfair because choice of law principles applicable to this action support the application of the common law of California to the nationwide common law claims of all Class members.

203. Additionally, given California's significant interest in regulating the conduct of businesses operating within its borders, and that California has the most significant relationship to Defendant as its highest number of pharmacies operate in California, there is no conflict in applying California law to non-resident, nationwide Class Members.

204. Alternatively, and/or in addition to California law, the laws set forth below apply to the conduct described herein.

COUNT I
Common Law Invasion of Privacy - Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Nationwide Class and, alternatively, the California Class)

205. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Nationwide Class and California Class.

206. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites

without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

207. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Digital Platforms and the communications platforms and services therein.

208. Plaintiff and Class Members communicated sensitive and protected medical information and individually identifiable health information that they intended for only Defendant to receive and that they understood Defendant would keep private and secure.

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

210. Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's Privacy Policy and other representations.

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

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

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

214. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to compensatory and/or nominal damages.

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

216. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

217. Plaintiff also seeks such other relief as the Court may deem just and proper.

COUNT II
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class and, alternatively, the California Class)

218. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Nationwide Class and California Class.

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

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

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

222. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Pixel (and other tracking technologies) to disclose and transmit Plaintiff's and Class Members' Private Information and the contents of their communications exchanged with Defendant to third parties.

223. The third-party recipients included, but were not limited to, Facebook and other online marketers.

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

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

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

a. Sensitive and confidential information that Plaintiff and Class Members

intended to remain private is no longer private;

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

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

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

e. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information and

f. Defendant's actions violated the property rights Plaintiff and Class Members have in their Private Information.

227. Plaintiff and Class Members are therefore entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation. Plaintiff is also entitled to punitive damages.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Nationwide Class and, alternatively, the California Class)

228. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Nationwide Class and California Class.

229. In light of the special relationship between Defendant Rite Aid and Plaintiff and Class Members, whereby Defendant Rite Aid became guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members

of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant Rite Aid did and does store.

230. Defendant Rite Aid has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant Rite Aid's relationship with its patients and former patients, in particular, to keep secure their Private Information.

231. Defendant Rite Aid breached its fiduciary duties to Plaintiff and Class Members by disclosing their Private Information to unauthorized third parties, and separately, by failing to notify Plaintiff and Class Members of this fact.

232. As a direct and proximate result of Defendant Rite Aid's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injury and are entitled to compensatory, nominal, and/or punitive damages, and disgorgement of profits, in an amount to be proven at trial.

COUNT IV
Negligence
(On Behalf of Plaintiff and the Nationwide Class and, alternatively, the California Class)

233. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Nationwide Class and California Class.

234. Defendant Rite Aid required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare/medical services.

235. By collecting and storing this data in Defendant Rite Aid's computer systems, Defendant had a duty of care to use reasonable means to secure and safeguard their computer systems—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from disclosure to third parties.

236. Defendant Rite Aid's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

237. Defendant Rite Aid owed a duty of care to Plaintiff and Class Members to provide

data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

238. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant Rite Aid and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law.

239. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

240. Defendant Rite Aid's duty to use reasonable security measures under HIPAA required Defendant Rite Aid to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

241. In addition, Defendant Rite Aid had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

242. Defendant Rite Aid's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

243. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant Rite Aid include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Plaintiff's and Class Members' Private Information;

d. Failing to detect in a timely manner that Plaintiff's and Class Members' Private Information had been compromised; and

e. Failing to timely notify—or notify at all—Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

244. It was foreseeable that Defendant Rite Aid's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members.

245. Plaintiff and Class Members are entitled to compensatory, nominal, and/or punitive damages.

246. Defendant Rite Aid's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner. Therefore, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant Rite Aid to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

COUNT V
Breach of Implied Contract
(*On Behalf of Plaintiff and the Nationwide Class and, alternatively, the California Class*)

247. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Nationwide Class and California Class.

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

249. Plaintiff and Class Members accepted Defendant's offers and provided their Private

Information to Defendant.

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

251. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information to third parties like Facebook.

252. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

253. Plaintiff and Class Members would not have used Defendant's services or would have paid substantially for these services, had they known their Private Information would be disclosed.

254. Plaintiff and Class Members are entitled to compensatory, consequential, and/or nominal damages as a result of Defendant's breaches of implied contract.

COUNT VI
Breach of Implied Covenant of Good Faith and Fair Dealing
(*On Behalf of Plaintiff and the Nationwide Class and, alternatively, the California Class*)

255. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Nationwide Class and California Class.

256. Plaintiff and Class Members entered into valid, binding, and enforceable implied contracts with Rite Aid, as alleged above.

257. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts.

258. These included the implied covenants that Rite Aid would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiff's and Class Members' Private Information and to comply with industry standards and federal and state laws and

regulations.

259. A "special relationship" exists between Rite Aid and the Plaintiff and Class Members. Rite Aid entered into a "special relationship" with Plaintiff and Class Members who sought healthcare services through Rite Aid and, in doing so, entrusted Rite Aid, pursuant to its requirements, with their Private Information.

260. Despite this special relationship with Plaintiff, Rite Aid did not act in good faith and with fair dealing to protect Plaintiff's and Class Members' Private Information.

261. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Rite Aid.

262. Rite Aid's failure to act in good faith in implementing the security measures required by the contracts denied Plaintiff and Class Members the full benefit of their bargain, and instead they received pharmacy prescription refills and related services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiff and Class Members were damaged in an amount at least equal to this overpayment.

263. Rite Aid's failure to act in good faith in implementing the security measures required by the contracts also caused Plaintiff and Class Members to suffer actual damages resulting from the disclosure and interception of their Private Information and they remain at imminent risk of suffering additional damages in the future.

264. Accordingly, Plaintiff and Class Members have been injured as a result of Rite Aid's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT VII
Unjust Enrichment
(*On Behalf of Plaintiff and the Nationwide Class and, alternatively, the California Class*)

265. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Nationwide Class and California Class.

266. Upon information and belief, Defendant Rite Aid funds its data security measures

entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

267. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant Rite Aid.

268. Plaintiff and Class Members conferred a monetary benefit on Defendant Rite Aid. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their Private Information.

269. In exchange, Plaintiff and Class Members should have received from Defendant Rite Aid the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

270. Defendant Rite Aid knew that Plaintiff and Class Members conferred a benefit which Defendant Rite Aid accepted. Defendant Rite Aid profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

271. In particular, Defendant Rite Aid enriched itself by obtaining the inherent value of Plaintiff's and Class Members' Private Information, and by saving the costs it reasonably should have expended on marketing and/or data security measures to secure Plaintiff's and Class Members' Private Information.

272. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant Rite Aid's decision to prioritize its own profits over the requisite security.

273. Under the principles of equity and good conscience, Defendant Rite Aid should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant Rite Aid failed to implement appropriate data management and security measures that are mandated by industry standards.

274. Defendant Rite Aid failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

275. If Plaintiff and Class Members knew that Defendant Rite Aid had not reasonably

secured their Private Information, they would not have agreed to provide their Private Information to Defendant Rite Aid.

276. Plaintiff and Class Members have no adequate remedy at law for this count. An unjust enrichment theory provides the equitable disgorgement of profits even where an individual has not suffered a corresponding loss in the form of money damage.

277. Furthermore, California law permits a standalone claim for unjust enrichment, allowing the court to construe the cause of action as a quasi-contract claim. *E.g., Astiana v. Hain Celestial Group, Inc*., 783 F.3d 753, 756 (9th Cir. 2015). California law recognizes a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss. *In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 599 (9th Cir. 2020). California law requires disgorgement of unjustly earned profits regardless of whether a defendant's actions caused a plaintiff to directly expend his or her own financial resources or whether a defendant's actions directly caused the plaintiff's property to become less valuable. Under California law, a stake in unjustly earned profits exists regardless of whether an individual planned to sell his or her data or whether the individual's data is made less valuable.

278. As a direct and proximate result of Defendant Rite Aid's conduct, Plaintiff and Class Members have suffered and will continue to suffer injury.

279. Defendant Rite Aid should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them, or to refund the amounts that Plaintiff and Class Members overpaid for Defendant Rite Aid's services.

COUNT VIII
Violations of Electronic Communications Privacy Act ("ECPA")
18 U.S.C. § 2511(1), *et seq*.
Unauthorized Interception, Use, and Disclosure
(On Behalf of Plaintiff and the Nationwide Class)

280. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the Nationwide Class.

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

282. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

283. The transmissions of Plaintiffs' PII and PHI to Defendant's Digital Platforms qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

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

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

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

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

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendant's web-servers; and

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

288. By utilizing and embedding the Pixel on its Digital Platforms, Defendant

intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

289. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Private Information to third parties such as Facebook.

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

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

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

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

294. The ECPA provides that a "party to the communication" may liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

295. Defendant is not a party for purposes to the communication based on its unauthorized duplication and transmission of communications with Plaintiff and the Class. However, even assuming Defendant is a party, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

296. Defendant's acquisition of patient communications that were used and disclosed to Facebook was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and individual States nationwide as set forth herein, including:

a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;

b. Invasion of privacy;

c. Breach of confidence;

d. Breach of fiduciary duty;

e. California Invasion of Privacy Act, §§ 630, *et seq*.;

f. California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56, et seq.;

297. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it: Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and disclosed individually identifiable health information to Facebook without patient authorization.

298. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

299. Defendant's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant's use of the Facebook source code was for Defendant's commercial advantage to increase revenue from existing patients and gain new patients.

300. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiff's and Class Members' communications about their Private Information on its Webpage, because it used its participation in these communications to improperly share Plaintiff's and Class members' Private Information with Facebook and third-parties that did not participate in these communications, that Plaintiff and Class Members did not know was receiving their information, and that Plaintiff and Class Members did not consent to receive this information

301. As such, Defendant cannot viably claim any exception to ECPA liability.

302. Plaintiff and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their PII and PHI (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiff and the Class members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiff's and the Class members' PII and PHI without providing any value or benefit to Plaintiff or the Class members;

c. Defendant received substantial, quantifiable value from its use of Plaintiff's and the Class Members' PII and PHI, such as understanding how people use its web properties and determining what ads people see on its web properties, without providing any value or benefit to Plaintiff or the Class Members;

d. Defendant has failed to provide Plaintiff and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and

e. The diminution in value of Plaintiff's and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, medical treatment, and appointments that Plaintiff and Class Members intended to remain private no longer private.

303. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiff's and Class Members' Private Information for financial gain.

304. Defendant was not acting under color of law to intercept Plaintiff's and the Class Members' wire or electronic communication.

305. Plaintiff and Class Members did not authorize Defendant to acquire the content of

their communications for purposes of invading their privacy via the Pixel.

306. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

307. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

308. As a result of Defendant's violation of the ECPA, Plaintiff and the Class are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT IX
Violations of the ECPA
18 U.S.C. § 2511(3)(a), *et seq*.
Unauthorized Divulgence by Electronic Communications Service
(On Behalf of Plaintiff & the Nationwide Class)

309. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the Nationwide Class.

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

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

312. Defendant's Website is an electronic communication service. The website provides to users thereof the ability to send or receive electronic communications. In the absence of

Defendant's Website, internet users could not send or receive communications regarding Plaintiff's and Class Members' PII and PHI.

313. Intentional Divulgence. Defendant intentionally designed the Pixel to, and was or should have been aware that, if misconfigured, it could divulge Plaintiff's and Class Members' PII and PHI.

314. While in Transmission. Upon information and belief, Defendant's divulgence of the contents of Plaintiff's and Class Members' communications was contemporaneous with their exchange with Defendant's Digital Platforms, to which they directed their communications.

315. Defendant divulged the contents of Plaintiff's and Class Members' electronic communications to third parties like Facebook without authorization.

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

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

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

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

d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency." 18 U.S.C. § 2511(3)(b).

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

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

> provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

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

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

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

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

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

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

COUNT X
Violation of the California Invasion of Privacy Act
Cal. Penal Code §§ 630, *et. seq.*
(On behalf of Plaintiff & the California Class)

324. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed California Class.

325. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to 638 ("CIPA").

326. The Act begins with its statement of purpose.

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

327. California Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or **who aids, agrees with, employs, or conspires** with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

(emphasis added).

328. Thus, a defendant must show that it had the consent of <u>all</u> parties to a communication.

329. At all relevant times, Defendant is and has been a "person" under CIPA, Cal. Penal Code § 631(a).

330. At all relevant times, Defendant aided, employed, agreed with, and conspired with third parties like Facebook to track and to intercept California Plaintiff's and Subclass Members' internet communications while accessing the Digital Platforms.

331. These communications were transmitted to and intercepted by a third party during the communications and without the knowledge, authorization, or consent of Plaintiff and Subclass Members.

332. Defendant intentionally implemented electronic technology into its Digital Platforms that, without the knowledge and consent of Plaintiff and Subclass Members, tracked and transmitted the substance of their confidential communications with Defendant to a third party.

333. Defendant willingly facilitated Facebook's and others' interception and collection of Plaintiff's and Subclass Members' Private Information by embedding the Pixel and other tracking technologies on its Digital Platforms. Defendant has full control over the Pixel, including which webpages contain the Pixel, what information is tracked and transmitted via the Pixel, and how events are categorized prior to their transmission.

334. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA:

a. The computer codes and programs Defendant used to track Plaintiff's and Subclass Members' communications while they were navigating the Digital Platforms;

b. Plaintiff's and Subclass Members' browsers;

c. Plaintiff's and Subclass Members' computing and mobile devices;

d. Defendant's web and ad servers;

e. The web and ad-servers from which Third Parties tracked and intercepted Plaintiff's and Subclass Members' communications while they were using a web browser to access or navigate the Digital Platforms;

f. The computer codes and programs used by third parties to effectuate the tracking and interception of Plaintiff's and Subclass Members' communications while they were using a browser to visit Defendant's Digital Platforms; and

g. The plan Defendant and others carried out to effectuate its tracking and

interception of Plaintiff's and Subclass Members' communications while they were using a web browser or mobile application to visit Defendant's Digital Platforms.

335. Based on these categories, the Pixel qualifies as a "machine[s], instrument[s], or contrivance[s]." At the very least, the Pixel falls under the broad catch-all category of "any other manner."

336. Defendant does not disclose that it is using Pixels specifically to track and automatically and simultaneously transmit communications to a third party.

337. Defendant is aware that these communications are confidential as its Privacy Policy and representations acknowledge the confidential nature of private medical information and disclaim that it is being shared with unidentified third parties without Plaintiff's and Subclass Members' express authorization.

338. The patient communication information that Defendant transmits while using Pixels constitutes protected health information.

339. By design, the Pixel transmits each of the user's actions taken on the webpage to a third party alongside and contemporaneously with the user initiating the communication.

340. Thus, user communication is intercepted in transit to the intended recipient—Defendant—before it reaches Defendant's server.

341. As demonstrated hereinabove, Defendant violates CIPA by aiding and permitting third parties to receive its patients' online communications in real time through its Digital Platforms without their consent.

342. By disclosing Plaintiff's and Subclass Members' Private Information, Defendant violated Plaintiff's and Subclass Members' statutorily protected right to privacy.

343. As a result of the above violations and pursuant to CIPA Section 637.2, Defendant is liable to Plaintiff and Subclass Members for the greater of: a) treble actual damages related to their loss of privacy in an amount to be determined at trial, or b) or for statutory damages in the amount of $5,000 per violation.

344. Cal. Penal Code Section 637.2 specifically states that "[it] is not a necessary

prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

345. Under the statute, Defendant is also liable for reasonable attorney fees, litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

COUNT XI
Violation of the California Confidentiality of Medical Information Act
Cal. Civ. Code §§ 56, *et seq*.
(On behalf of Plaintiff & the California Class)

346. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed California Class.

347. The California Confidentiality of Medical Information Act, California Civil Code §§ 56, *et seq.* ("CMIA") prohibits health care providers from disclosing medical information relating to their patients without patient authorization. "Medical information" refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care . . . regarding a patient's medical history, mental or physical condition, or treatment. 'Individually Identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual[.]" Cal. Civ. Code § 56.05.

348. Defendant is a "provider of health care" as defined by California Civil Code § 56.06(b) and is, therefore, subject to the requirements of the CMIA, including, but not limited to, §§ 56.10 and 56.101.

349. Cal. Civil Code § 56.10 states, in pertinent part, that "[n]o provider of health care . . . shall disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization . . . ."

350. Section 56.101 of the CMIA states, in pertinent part, that "[a]ny provider of health care . . . or contractor . . . who negligently creates, maintains, preserves, stores, abandons, destroys,

or disposes of medical information shall be subject to the remedies and penalties . . ." Cal. Civ. Code §§ 56.10, 56.101.

351. Plaintiff and Subclass Members are patients, and, as a health care provider, Defendant has an ongoing obligation to comply with the CMIA's requirements.

352. As set forth above, device identifiers, web URLs, Internet Protocol (IP) addresses, and other characteristics that can uniquely identify Plaintiff and Subclass Members are transmitted to Defendant in combination with patient medical conditions, medical concerns, treatment(s) sought by the patients, medical history, appointment information, and other medical information. This is protected health information under the CMIA.

353. This private medical information is intercepted and transmitted to Facebook and other third parties via Defendant's knowing and intentional decision to embed enabling software into its Digital Platforms.

354. Facebook ID is also an identifier sufficient to allow identification of an individual. Along with patients' Facebook ID, Defendant discloses to Facebook several pieces of information regarding patient use of its Web Properties including, but not limited to, the following: patient medical conditions, medical concerns, treatment(s) sought by the patients, medical specialty of the doctor(s) searched for and selected by patients, and appointment information.

355. Upon information and belief, the private medical information of Plaintiff and Subclass Members that was improperly intercepted and transmitted to third parties like Facebook via Defendant's use of the Pixel was subsequently improperly viewed, accessed, acted upon, and otherwise used by third parties to, among other things, tailor advertisements to them based on their medical conditions and other private medical information for gain.

356. The information described above constitutes medical information pursuant to the CMIA because it is patient information derived from a provider of health care regarding patients' medical treatment and physical condition, and this medical information is linked with individually identifying information. Cal. Civ. Code § 56.05(i).

357. As demonstrated herein, Defendant fails to obtain its patients' authorization for the disclosure of medical information and fails to disclose in its Web Properties Notice of Privacy

Practices that it shares protected health information with Facebook or other third parties for marketing purposes.

358. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical information must be:

> (1) Clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization;
>
> (2) signed and dated by the patient or patient representative;
>
> (3) state the name and function of the third party that receives the information and
>
> (4) state a specific date after which the authorization expires.

359. Further, Defendant's Website Notice of Privacy Practices does not require consumers to agree to the terms by selecting or clicking a "checkbox" presented in a sufficiently conspicuous manner to put Plaintiff on notice of them. Accordingly, the information set forth in Defendant's Website Privacy Notice does not qualify as a valid authorization.

360. As described above, Defendant is violating the CMIA by disclosing its patients' medical information to third parties along with the patients' individually identifying information.

361. Accordingly, Plaintiff and Subclass Members seek all available relief including nominal damages, compensatory damages, punitive damages, attorney fees, and costs of litigation for Defendant's violation(s) of the CMIA.

COUNT XII
Invasion of Privacy Under California's Constitution
Cal. Const. Art. 1, § 1
(*On Behalf of Plaintiff & the California Class*)

362. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed California Class.

363. Article I, section 1 of the California Constitution provides that "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

364. The right to privacy in California's constitution creates a private right of action against private and government entities.

365. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy, and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

366. Defendant Rite Aid violated Plaintiff's and Subclass Members' constitutional right to privacy by collecting, storing and disclosing their personal information in which they had a legally protected privacy interest and for which they had a reasonable expectation of privacy, in a manner that was highly offensive to Plaintiff and Subclass Members and was an egregious violation of social norms.

367. Defendant Rite Aid has intruded upon Plaintiff's and Subclass Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential Personal Information.

368. Plaintiff and Subclass Members had a reasonable expectation of privacy in that: (i) Defendant's invasion of privacy occurred as a result of Defendant's security practices, including the collecting, storage, and unauthorized disclosure of consumers' personal information; (ii) Plaintiff and Subclass Members did not consent to or otherwise authorize Defendant Rite Aid to disclosure their personal information; and (iii) Plaintiff and Subclass Members could not reasonably expect Defendant would commit acts in violation of privacy protection laws.

369. As a direct and proximate result of Defendant Rite Aid's invasion of their privacy, Plaintiff and Subclass Members have been damaged and have suffered actual and concrete injuries.

370. Plaintiff and Subclass Members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, risk of future invasions of privacy and the mental and emotional distress and harm to human dignity interests caused by Defendant Rite Aid's invasions.

371. Plaintiff and Subclass Members seek appropriate relief for that injury including, but not limited to, damages that will reasonably compensate Plaintiff and Subclass Members for the

harm to their privacy interests, nominal damages, and/or disgorgement of profits made by Defendant Rite Aid as a result of its intrusions upon Plaintiff's and Class Members' privacy.

COUNT XIII
Violation of The California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful and Fraudulent Business Practices
(On Behalf of Plaintiff & the California Class)

372. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed California Class.

373. Plaintiff, Subclass Members, and Defendant are each a "person" under Cal. Bus. & Prof. Code § 17201.

374. The acts, omissions, and conduct of Defendant as alleged herein constitute "business practices" within the meaning of the UCL.

375. California Business and Professions Code §§ 17201, et seq. prohibits acts of unfair competition, which includes unlawful business practices.

376. Plaintiff brings her claims for injunctive relief as she has no confidence that Defendant has altered its privacy practices and she may wish to use Defendant's services in the future.

377. Plaintiff brings her claims for restitution in the alternative to her claims for damages.

378. Defendant's business acts and practices are "unlawful" under the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et. seq.* because, as alleged above, Defendant violated California common law, the California Constitution, and other statutes and causes of action alleged herein.

379. Defendant engaged in unlawful business practices by disclosing Plaintiff's and Subclass Members' Private Information to unrelated third parties, including Facebook, by imbedding the Pixel on its Digital Platforms without prior consent in violation of the consumer protection and privacy statutes alleged herein, including the following: California Constitution, Article I, section 1; Cal. Penal Code §§ 630, *et. seq.*; Cal. Civ. Code §§ 56, *et. seq.*; 18 U.S.C. § 2511(1), *et seq.*; 18 U.S.C. § 2511(3)(a), *et seq.*; Section 5 of the FTC Act, 15 U.S.C 45, et seq.; and the HIPAA violations set forth above.

380. Because Defendant is in the business of providing healthcare services, Plaintiff and Subclass Members relied on Defendant to advise them of any potential disclosure of their Private Information. Plaintiff and Subclass Members understood that Defendant, as a healthcare provider, would take appropriate measures to keep their Private Information private and confidential.

381. In its privacy policies, Defendant promised that it would not share Plaintiff's and Subclass Members' Private Information with any third party without consent or for marketing purposes. Contrary to its own policies, Rite Aid did disclose Plaintiff's and Subclass Members' Private Information to third parties without consent and for marketing purposes.

382. Had Defendant disclosed that it shared Private Information with third parties, Plaintiff would have been aware of the disclosure, and would not have used Defendant's services or would have paid considerably less for those services.

383. As a direct and proximate result of Defendant's violations of the UCL, Plaintiff and Subclass Members have suffered injury in fact and lost money or property, including, but not limited to, payments Plaintiff and Subclass Members made to Defendant and/or other valuable consideration, in addition to the exposure of their Private Information. Plaintiff and Subclass Members also lost the value of their Private Information as a result of Defendant's unlawful disclosures.

384. Plaintiff and Subclass Members also face a real and immediate threat of future injury to the confidentiality of their Private Information because such information remains within Defendant's control and because anytime that Plaintiff and Subclass Members interact with the Digital Platforms to make appointments, submit information about their medical conditions, search for doctors, or otherwise seek assistance related to their medical conditions, Plaintiff and Subclass Members risk further disclosure of their Private Information. Plaintiffs continue to want to use Rite Aid's Digital Platforms and would resume using Rite Aid's services if Rite Aid complies with applicable laws and stops using the Pixel on its Digital Platforms. Plaintiff and Subclass Members are, therefore, entitled to injunctive relief, requiring that Defendant cease all website operations that allow for the third-party capture of Private Health Information.

385. As a direct result of its unlawful and deceptive practices, Defendant has been unjustly

enriched and should be required to make restitution to Plaintiff and to Subclass Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code, restitutionary disgorgement of all profits accruing to Defendant because of its unlawful business practices, declaratory relief, attorney fees, and costs of litigation (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

386. In the alternative to those claims seeking remedies at law, Plaintiff and Subclass Members allege that there is no plain, adequate, and complete remedy that exists at law to address Defendant's unlawful and unfair business practices.

387. The legal remedies available to Plaintiff are inadequate because they are not "equally prompt and certain and in other ways efficient" as equitable relief. *American Life Ins. Co. v. Stewart*, 300 U.S. 203, 214 (1937); *see also United States v. Bluitt*, 815 F. Supp. 1314, 1317 (N.D. Cal. Oct. 6, 1992) ("The mere existence' of a possible legal remedy is not sufficient to warrant denial of equitable relief.").

388. Additionally, unlike damages, the Court's discretion in fashioning equitable relief is very broad and can be awarded in situations where the entitlement to damages may prove difficult. *Cortez v. Purolator Air Filtration Products Co.*, 23 Cal.4th 163, 177-180 (2000) (Restitution under the UCL can be awarded "even absent individualized proof that the claimant lacked knowledge of the overcharge when the transaction occurred.").

389. Thus, restitution would allow recovery even when normal consideration associated with damages would not. *See, e.g., Fladeboe v. Am. Isuzu Motors Inc.*, 150 Cal. App. 4th 42, 68 (2007) (noting that restitution is available even in situations where damages may not be available). Furthermore, the standard for a violation of the UCL "unlawful" prong is different from the standard that governs legal claims.

COUNT XIV
Violation of the UCL
Cal. Bus. & Prof. Code § 17200, *et seq*.- Unfair Business Practices
(On behalf of Plaintiff & the California Class)

390. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed California Class.

391. Defendant's business acts and practices meet the unfairness prong of the UCL according to all three theories of unfairness.

392. First, Defendant's business acts and practices are "unfair" under the UCL pursuant to the three-part test articulated in *Camacho v. Automobile Club of Southern California* (2006) 142 Cal. App. 4th 1394, 1403: (a) Plaintiff and Subclass Members suffered substantial injury due to Defendant's disclosure of their Private Information; (b) Defendant's disclosure of Plaintiff's and Class Members' Private Information provides no benefit to consumers, let alone any countervailing benefit that could justify Defendant's disclosure of Private Information without consent for marketing purposes or other pecuniary gain; and (c) Plaintiff and Subclass Members could not have readily avoided this injury because they had no way of knowing that Defendant was implementing the Pixel. Thus, Plaintiff and Subclass Members did not know to ask Defendant to stop the practice of disclosing their Private Information and did not know that they should stop using Defendant's services to avoid disclosing their Private Information

393. Second, Defendant's business acts and practices are "unfair" under the UCL because they are "immoral, unethical, oppressive, unscrupulous, or substantially injurious" to Plaintiff and Subclass Members, and "the utility of [Defendant's] conduct," if any, does not "outweigh the gravity of the harm" to Plaintiff and Subclass Members. *Drum v. San Fernando Valley Bar Ass'n*, (2010) 182 Cal. App. 4th 247, 257. Defendant engaged in unfair business practices by disclosing Plaintiff's and Subclass Members' Private Information to unrelated third parties, including Facebook, without prior consent despite its promises to keep such information confidential. This surreptitious and undisclosed conduct is immoral, unethical, oppressive, unscrupulous, and substantially injurious. No benefit inheres in this conduct, the gravity of which is significant.

394. Third, Defendant's business acts and practices are "unfair" under the UCL because they run afoul of "specific constitutional, statutory, or regulatory provisions." *Drum*, 182 Cal. App. 4th at 256 (internal quotation marks and citations omitted). California has a strong public policy of protecting consumers' privacy interests, including consumers' and patients' personal data. This public policy is codified in California's Constitution in Article I, section 1; CIPA, Cal. Penal Code §§ 630, *et seq.*; the CMIA, Cal. Civil Code §§ 56.06, 56.10, 56.101; the California Consumer

Privacy Act, Cal. Civil Code §§ 1798, *et seq.*; and the California Consumer Records Act, Cal. Civil Code § 1798.81.5, among other statutes.

395. This public policy is further codified on a nationwide basis in federal statutes, including HIPAA, FTC Act, and the ECPA. Defendant violated this public policy by, among other things, surreptitiously collecting, disclosing, and otherwise exploiting Plaintiff's and Subclass Members' Private Information by sharing it with Facebook and other third parties via the Pixel without Plaintiff's and/or Subclass Members' consent.

396. Because Defendant is in the business of providing healthcare services, Plaintiff and Subclass Members relied on Defendant to advise them of any potential disclosure of their Private Information.

397. Plaintiff and Subclass Members understood that Defendant, as a healthcare provider, would take appropriate measures to keep their private information private and confidential.

398. In its privacy policies, Defendant promised that it would not share Plaintiff's and Subclass Members' private information with any third party without consent or for marketing purposes. Contrary to its own policies, Rite Aid did disclose Plaintiff's and Subclass Members' Private Information to third parties without consent and for marketing purposes. Defendant was in sole possession of and had a duty to disclose the material information that Plaintiff's and Subclass Members' Private Information was being shared with a third party.

399. Had Defendant disclosed that it shared Private Information with third parties, Plaintiff would not have used Defendant's services or would have paid considerably less for those services.

400. The harm caused by the Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests other than Defendant's conduct described herein.

401. Plaintiff and Subclass Members trusted Defendant to keep their Private Information confidential, and as a result, shared highly sensitive information through their use of the Digital Platforms, causing them to suffer damages when Defendant disclosed that information to a third party.

402. As a direct and proximate result of Defendant's violations of the UCL, Plaintiff and Subclass Members have suffered injury in fact and lost money or property, including, but not limited to, payments Plaintiff and Subclass Members made to Defendant and/or other valuable consideration, such as access to their private and personal data. Plaintiff and Subclass Members also lost the value of their Private Information as a result of Defendant's unfair business practices.

403. As a direct result of its unfair practices, Defendant has been unjustly enriched and should be required to make restitution to Plaintiff and Subclass Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code, restitutionary disgorgement of all profits accruing to Defendant because of its unlawful business practices, declaratory relief, attorney fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

404. In the alternative to those claims seeking remedies at law, Plaintiff and Subclass Members allege that there is no plain, adequate, and complete remedy that exists at law to address Defendant's unlawful and unfair business practices. The legal remedies available to Plaintiff are inadequate because they are not "equally prompt and certain and in other ways efficient" as equitable relief. *American Life Ins. Co. v. Stewart*, 300 U.S. 203, 214 (1937); *see also United States v. Bluitt*, 815 F. Supp. 1314, 1317 (N.D. Cal. Oct. 6, 1992) ("The mere existence' of a possible legal remedy is not sufficient to warrant denial of equitable relief.").

405. Additionally, unlike damages, the Court's discretion in fashioning equitable relief is very broad and can be awarded in situations where the entitlement to damages may prove difficult. *Cortez v. Purolator Air Filtration Products Co.*, 23 Cal.4th 163, 177-180 (2000) (Restitution under the UCL can be awarded "even absent individualized proof that the claimant lacked knowledge of the overcharge when the transaction occurred.").

406. Thus, restitution would allow recovery even when normal consideration associated with damages would not. *See, e.g., Fladeboe v. Am. Isuzu Motors Inc.*, 150 Cal. App. 4th 42, 68 (2007) (noting that restitution is available even in situations where damages may not be available). Furthermore, the standard for a violation of the UCL "unfair" prong is different from the standard that governs legal claims.

COUNT XV

Violation of the California Consumer Privacy Act ("CCPA")
Cal. Civ. Code §§ 1798, *et seq.*
(On behalf of Plaintiff & the California Class)

407. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed California Class.

408. The CCPA, Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
>
> (B) Injunctive or declaratory relief.
>
> (C) Any other relief the court deems proper.

409. Defendant Rite Aid is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

410. Plaintiff and Subclass Members are covered "consumers" under subdivision (g) of § 1798.140 in that they are natural persons who are California residents.

411. The personal information of Plaintiff and Subclass Members at issue in this lawsuit constitutes "personal information" under subdivision (a) of § 1798.150 and § 1798.81.5, in that the personal information Defendant Rite Aid collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) driver license number, California

identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

412. Defendant Rite Aid knew or should have known that the Pixel embedded on its Digital Platforms disclosed Plaintiff's and Subclass Members' Private Information without authorization.

413. Defendant Rite Aid subjected Plaintiff's and the Subclass Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant Rite Aid's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

414. As a direct and proximate result of Defendant Rite Aid's conduct, Plaintiff and the Subclass Members were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

415. Section 1798.150(b) specifically provides that: "[n]o[prefiling]notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages." Accordingly, Plaintiff and the Subclass Members, by way of this complaint, seek actual pecuniary damages suffered as a result of Defendant Rite Aid's violations described herein. Plaintiff has issued and/or will issue a notice of these alleged violations pursuant to subdivision (b) of § 1798.150 and intends to amend this complaint to seek statutory damages and injunctive relief upon expiration of the 30-day cure period pursuant to subdivsions (a)(1)(A)-(B), (a)(2), and (b) of § 1798.

COUNT XVI
Violation of California Customer Records Act
Cal. Civ. Code § 1798.81.5
(On behalf of Plaintiff & the California Class)

416. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed California Class.

417. The California Customer Records Act, Cal. Civ. Code § 1798.81.5 (all further statutory references in this count are to the California Civil Code), provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

418. Subdivision (b) of § 1798.81.5 further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

419. Subdivision (b) of § 1798.84 provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Subdivision (e) of § 1798.84 further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

420. Plaintiff and Subclass Members are "customers" within the meaning of subdivision (c) of § 1798.80 and subdivision (b) of § 1798.84 because they are individuals who provided personal information to Defendant Rite Aid, directly and/or indirectly, for the purpose of obtaining a service from Defendant Rite Aid.

421. The personal information of Plaintiff and Subclass Members at issue in this lawsuit constitutes "personal information" under subdivision (d)(1) of § 1798.81.5 in that the personal information Defendant Rite Aid collects and which was impacted by Defendant's unlawful disclosures includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) driver license number, California

identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

422. Defendant Rite Aid knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Subclass Members' personal information and that the risk of disclosure was highly likely. Defendant Rite Aid failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and Subclass Members. Specifically, Defendant Rite Aid intentionally disclosed Plaintiff's and Class Members' Private Information and/or failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and Subclass Members from unauthorized access, destruction, use, modification, or disclosure. Defendant Rite Aid further subjected Plaintiff's and Subclass Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of its conduct.

423. As a direct and proximate result of Defendant Rite Aid's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and Subclass Members included unauthorized access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and Subclass Members by unauthorized third parties.

424. As a direct and proximate result of Defendant Rite Aid's acts or omissions, Plaintiff and Subclass Members were injured and lost money or property including, but not limited to, the loss of Plaintiff's and Subclass Members' legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to subdivision (b) of § 1798.84.

425. Section § 1798.82 further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

426. Any person or business that is required to issue a security breach notification under the California Customer Records Act must meet the following requirements under subdivision (d) of § 1798.82:

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

i. the date of the breach,
ii. the estimated date of the breach, or
iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

427. Defendant failed to provide the legally compliant notice under subdivision (d) of §

1798.82 to Plaintiff and Subclass Members. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to Plaintiff and Subclass Members.

428. On information and belief, Subclass Members affected by the breach have not received any notice at all from Defendant Rite Aid in violation of subdivision (d) of § 1798.82.

429. As a result of the violations of § 1798.82, Plaintiff and Subclass Members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and other Class Members, prays for judgment against Defendant as follows:

A. an Order certifying the Nationwide Class and California Class, and appointing the Plaintiff and her Counsel to represent the Classes;

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

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

D. an award of all damages available at equity or law, including, but not limited to, actual, consequential, punitive, statutory and nominal damages, as allowed by law in an amount to be determined;

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

F. prejudgment interest on all amounts awarded and

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

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and other members of the Classes, hereby demands a jury trial on all issues so triable.

Dated: July 19, 2023

Respectfully Submitted,

/s/ *Adam B. Wolf*

Adam B. Wolf (Cal. Bar No. 215914)
PEIFFER WOLF CARR KANE
CONWAY & WISE LLP
3435 Wilshire Blvd., Ste. 1400
Los Angeles, CA 90010
Telephone: (415) 766-3545
Facsimile: (415) 840-9435
awolf@peifferwolf.com

Brandon M. Wise*
PEIFFER WOLF CARR KANE
CONWAY & WISE LLP
818 Lafayette Ave., Floor 2
St. Louis, MO 63104
Tel: 314-833-4825
bwise@peifferwolf.com

Andrew R. Tate*
PEIFFER WOLF CARR KANE
CONWAY & WISE LLP
235 Peachtree St. NE, Suite 400
Atlanta, GA 30303
Telephone: 314.669.3600
atate@peifferwolf.com

David S. Almeida*
Elena A. Belov*
ALMEIDA LAW GROUP LLC
849 W Webster Avenue
Chicago, IL 60614
Telephone: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

Attorneys for Plaintiff & the Putative Classes

** Pro Hac Vice forthcoming*

ClassAction.org
