IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

PATRICK MILLER, individually and on behalf of similarly situated individuals, *Plaintiff*, v. UNIVERSITY OF COLORADO HEALTH *Defendant.*	)	Case No. 26-cv-3562 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Patrick Miller ("Plaintiff"), individually and on behalf of other similarly situated individuals, brings this Class Action Complaint against Defendant University of Colorado Health ("UC Health" or "Defendant") to stop Defendant's intentional and unlawful disclosure of its patients' confidential personally identifiable information and protected health information (collectively "Private Information") and to seek redress for all those who have been harmed by Defendant's misconduct. Plaintiff alleges as follows based on personal knowledge as to himself and his own acts and experiences and as to all other matters, on information and belief, including an investigation by his attorneys.

THE PARTIES

1. Plaintiff Patrick Miller is a natural person, resident, and a citizen of Larimer County, Colorado. Plaintiff is a patient with UC Health and has used the UC Health website and patient portal.

2. Defendant UC Health is a Colorado non-profit hospital headquartered in Aurora, Colorado. UC Health System includes a network of hospitals, medical centers, and clinics throughout Colorado.

JURISDICTION AND VENUE

3. This Court has subject-matter jurisdiction under 28 U.S.C. § 1331 because this case arises under the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq*.

4. Jurisdiction and Venue are proper in this judicial district under 28 U.S.C. §§ 1391(b)(1), (b)(2), and (c)(2) as Defendant is headquartered in this District, resides in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred here.

INTRODUCTION

5. Plaintiff brings this action to seek redress for Defendant's intentional interception and disclosure of Plaintiff's and Class Members' confidential personally identifiable information and protected health information through Defendant's implementation and use of the Meta/Facebook tracking pixel on its website, including Defendant's "Find a Doctor" tool. Upon information and belief, Defendant engaged in materially the same conduct through its "My Health Connection" patient portal.

6. Defendant's Find a Doctor tool allows patients and prospective patients to search for physicians, specialties, providers, clinics, appointments, procedures, symptoms, and medical conditions. Defendant configured its website to cause the contents of those communications to be contemporaneously duplicated and transmitted to Meta/Facebook, together with identifying information such as IP addresses, device identifiers, browser identifiers, cookie identifiers, and/or Facebook-linked identifiers.

7. Defendant's website also provides patients with access to "My Health Connection," a patient portal built on the Epic Systems MyChart platform, through which patients and authorized users can, among other things, send and receive secure messages with their healthcare providers, view laboratory and test results, view diagnoses and clinical notes, request prescription refills, and review or schedule appointments. Upon information and belief, Defendant implemented and configured the Meta/Facebook Tracking Pixel and/or similar tracking technology (together, "Tracking Pixel") on some or all pages of the My Health Connection patient portal.

8. Plaintiff and Class Members are individuals who used Defendant's Find a Doctor tool to search for providers, specialties, clinics, appointments, symptoms, procedures, and/or treatment for specific medical conditions, and whose communications were intercepted, redirected, and disclosed to Meta/Facebook without their knowledge, consent, or authorization. Plaintiff and Class Members also include individuals who used Defendant's My Health Connection patient portal, whose communications were, upon information and belief, likewise intercepted, redirected, and disclosed to Meta/Facebook or other third parties without their knowledge, consent, or authorization.

9. Information about an individual's mental and physical health is among the most sensitive information in our society, and strict protection is essential because unauthorized disclosure can result in severe repercussions, including social stigma, workplace discrimination, and denial of insurance coverage.

10. Plaintiff and Class Members reasonably believed that their communications with Defendant through the Find a Doctor tool were private and confidential. Instead, Defendant embedded and configured the Meta/Facebook Tracking Pixel on the Find a Doctor tool, causing Plaintiff's and Class Members' communications to be secretly duplicated and transmitted to

Meta/Facebook. These transmissions included the substance of Plaintiff's and Class Members' healthcare-related communications with Defendant, including searches for providers, specialties, symptoms, procedures, treatment, clinics, appointment-related information, and/or medical conditions, together with identifiers that could be used to connect those communications to a specific person.

11. A pixel is a piece of code that "tracks the people and the types of actions they take" as they interact with a website.[1]

12. The user's web browser executes the pixel via instructions within the webpage to communicate certain information based on criteria selected by the website's owner. The website owner controls which of its pages contain the Pixel and which actions are tracked and transmitted to Facebook.

13. Defendant utilized the Tracking Pixel for marketing purposes. Pixels gather data about a person, build a profile for them based on their search activity, and utilize that data to retarget future marketing efforts with specialized advertisements in an effort to bolster profits.

14. The information that Defendant's Tracking Pixel sent to Meta/Facebook included the contents of Plaintiff's and Class Members' communications with Defendant through the Find a Doctor tool, including, for example, search terms, selected specialties, provider names, clinic pages, condition-specific queries, procedure-related searches, insurance-related selections, zip codes, appointment-related clicks, page URLs, referrer URLs, event data, button-click data, and other information reflecting the substance, purpose, and meaning of the user's healthcare-related communication with Defendant.

[1] https://www.facebook.com/business/goals/retargeting

15. This information allowed Meta/Facebook to know that an identified or identifiable person communicated with Defendant about specific healthcare providers, specialties, symptoms, conditions, procedures, appointments, or treatment. Defendant used the Tracking Pixel to obtain marketing, analytics, advertising, retargeting, patient-acquisition, and/or cost-saving benefits from those intercepted communications.

16. Healthcare patients do not have reason to suspect that their trusted healthcare provider will send confidential medical information collected via its webpages to an unknown third party without the patient's consent. Plaintiff and the other Class Members never consented to, agreed to, authorized, or otherwise permitted UC Health to disclose their Private Information.

17. Defendant has never disclosed to Plaintiff or Class Members that it covertly transmitted their sensitive and confidential information to Facebook as they communicated with their healthcare provider via the Find a Doctor tool.

18. Defendant further made express and implied promises to Plaintiff and Class Members to protect their Private Information and maintain the confidentiality of communications that patients exchanged with Defendant on the UC Health website.

19. The disclosure of Plaintiff's and Class Members' Private Information via the Pixel violates the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which governs how health care providers must safeguard patients' Private Information.

20. HIPAA and its implementing regulations prohibit covered entities such as Defendant from disclosing individually identifiable health information and protected health information to third parties for marketing, advertising, analytics, retargeting, or other non-treatment purposes without a valid authorization or other legally recognized basis for disclosure.

21. Defendant assumed legal, statutory, regulatory, contractual, and equitable duties to Plaintiff and Class Members to protect the confidentiality of their healthcare-related communications and to refrain from disclosing their personally identifiable information and protected health information to unauthorized third parties.

22. Defendant failed to honor those duties by intentionally installing, configuring, and maintaining tracking technology on the Find a Doctor tool that caused Plaintiff's and Class Members' confidential healthcare communications and identifying information to be intercepted, redirected, and transmitted to Meta/Facebook without their knowledge, consent, or authorization.

23. Plaintiff's and Class Members' Private Information can—and likely will—be further exploited for retargeting or marketing, or by insurance companies utilizing the information to set insurance rates.

24. Defendant breached its statutory and common law obligations to Plaintiff and Class Members by, *inter alia*: (i) failing to adequately review its Find a Doctor tool to ensure that it operated safely and securely; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) aiding, agreeing, and working with third-parties to intercept communications sent and received by Plaintiff and Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook or other third party technology vendors; (v) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Tracking Pixels; (vi) failing to warn Plaintiff and Class Members; and (vii) otherwise failing to design and monitor its website to maintain the confidentiality and integrity of patient Private Information.

25. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy, (ii) lost time and opportunity costs

associated with attempting to mitigate the actual consequences of the Tracking Pixel, (iii) loss of benefit of the bargain, (iv) diminution or deprivation of value of the Private Information, (v) statutory damages, and (vi) the continued and ongoing risk of exposure of their Private Information.

26. Plaintiff seeks to remedy these harms and brings this suit for Violation of the Electronic Communications Privacy Act.

COMMON FACTUAL ALLEGATIONS

A. Facebook's (Meta) Tracking Tools

27. Facebook runs the world's largest social media company, generating well over $100 billion from the sale of advertising space viewed by social media users each year.

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

29. The Business Tools are automatically configured to capture data created by the visitor's interactions, including "Standard Events" such as when a user visits a particular webpage, the webpage's URL, metadata, button clicks, and other information.

30. Businesses that want to target customers and advertise their services, such as UC Health, can track other visitor actions and can create their own tracking parameters by building a "custom event."[2]

31. Facebook's pixel is one of the most widely distributed website trackers on the internet that "tracks people and the actions they take" while they visit a website.

32. When a visitor accesses a webpage that is hosting the Facebook Tracking Pixel, the

[2] https://www.facebook.com/business/help/964258670337005?id=1205376682832142

communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook, traveling from the visitor's browser to Facebook's servers.

33. The Facebook pixel's primary purpose is for marketing, ad targeting, and an increase in sales generation.[3]

34. Meta Pixel can collect and transmit, among other things, the following data:

a. **HTTP Headers:** HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document referrer, and other information.

b. **Pixel-specific data:** Includes Pixel ID and Facebook Cookies.

c. **Button Click Data:** Includes any buttons clicked by site visitors, the labels of those buttons and any pages visited from the button clicks.

d. **Optional Values:** Developers and marketers can optionally choose to send additional information about the visit through Custom Data events. Examples of custom-data events include conversion value, page type and more.

e. **Form Field Names:** Includes website field names like email, address, quantity, etc., for when you purchase a product or service.

35. Facebook also advertises to prospective users (*i.e.*, website owners) that Meta Pixel can be used to:

1. Make sure ads are shown to the right people by finding new customers or people who have visited a specific page on the website.

[3] https://developers.facebook.com/documentation/meta-pixel

2. Drive more sales by reaching people who are more likely to take an action you care about, like making a purchase.

3. Measure the impact of ads by measuring what happens when people see them.

36. Critically, a website visitor's Facebook Profile ID, or FID, is directly linked to their Facebook profile, which includes a wide range of demographics and information about the user, including pictures, work history, personal interests, and their relationships. Meta—or any ordinary person—can use the Facebook Profile ID to quickly locate, access, and view the user's Facebook profile.

37. By incorporating the Meta/Facebook Tracking Pixel on its Find a Doctor tool, Defendant caused Meta/Facebook to receive Plaintiff's and Class Members' healthcare-related communications together with identifying information, including IP addresses, device identifiers, browser identifiers, cookie identifiers, and/or Facebook-linked identifiers. This identifying information could be used, alone or in combination with other information, to connect the healthcare-related communication to a specific person.

38. Meta also offers server-side tracking technology, including its Conversions API, which allows website owners to transmit event data directly from their servers to Meta. To the extent Defendant used server-side tracking, Conversions API, or any similar technology, those tools further enabled Defendant to transmit patient communications and related identifying information to Meta without relying solely on the patient's browser.

39. Upon information and belief, Defendant's tracking tools were configured to transmit event data and other information reflecting user interactions with Defendant's Find a Doctor tool, including page views, searches, selections, button clicks, appointment-related events, provider-page views, specialty searches, condition-related searches, and/or other healthcare-

related communications.

40. Without permission from Plaintiff or Class Members, Defendant used tracking technology to commandeer patients' browsers and/or website communications, causing their communications with Defendant to be contemporaneously redirected, duplicated, and transmitted to Meta/Facebook.

B. Defendant Utilizes Facebook's Tracking Pixel

41. A technical analysis of Defendant's Find a Doctor webpage revealed that Defendant implemented, during the relevant time period, Facebook's Tracking Pixel to track visitors.

42. Upon information and belief, Defendant also implemented Facebook's Tracking Pixel and/or similar tracking technology on some or all pages of its My Health Connection patient portal. This belief is based on, among other things: (a) public reporting that a substantial number of hospital systems nationwide — including systems operating on the same Epic/MyChart patient-portal platform used by Defendant — have implemented the Meta/Facebook Tracking Pixel or similar tracking technology within password-protected patient portals; and (b) Defendant's demonstrated practice, confirmed by technical analysis, of using the Tracking Pixel on other patient-facing pages of its website, including the Find a Doctor tool. The precise nature, scope, and duration of Defendant's use of tracking technology on the patient portal is a matter peculiarly within Defendant's knowledge, custody, and control and is properly the subject of discovery.

43. When a visitor visits Defendant's website and clicks on the "Find a Doctor" tab, the individual's browser sends a request to Defendant's server requesting that it load the webpage. Because Defendant's website utilizes the Tracking Pixel, Facebook's embedded code sends secret instructions back to the individual's browser, causing the browser to secretly duplicate the communication with Defendant and transmit it to Facebook's servers, alongside additional

information that transcribes the communication's content and the individual's identity.

44. For example, if the user clicks "Find a Doctor" and enters a zip code, selects an insurance company, and searches for a particular specialty, like "Addiction Psychiatry," or uses another search term to find a doctor, such as "heart disease," this information is shared with third parties that UC Health has configured its pixels to interact with.

45. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into datasets to be used by Defendant for website improvement and marketing purposes.

46. Furthermore, every time Defendant sends a patient's website activity data to Facebook, that patient's PII is also disclosed, including their Facebook ID, User ID, or Client ID. Critically, Facebook or any ordinary person who comes into possession of a Facebook ID can easily identify any individual on its platform with only their unique ID.

47. Rather than configuring its tracking software to limit the information that it communicated to third parties, Defendant instead intentionally selected the features and functionality of the Tracking Pixel that resulted in disclosure of its patients' Private Information.

48. As such, Defendant intercepted and disclosed to Facebook Plaintiff's and Class Members' Private Information including their: (1) status as medical patients; (2) health conditions; (3) treatment and therapies; (4) communications with Defendant through its website; (5) information about their specific medical providers and related information; (6) the webpages that they viewed; and (7) phrases entered as search queries to obtain specific information about a specific doctor and symptoms they are experiencing.

49. Plaintiff and Class Members did not intend or have any reason to suspect the Private Information would be shared with Facebook, or that Defendant was tracking their every

communication and disclosing the same to third parties when they entered highly sensitive information on Defendant's website. Plaintiff and Class Members never consented to, agreed to, authorized, or otherwise permitted Defendant to disclose their Private Information.

50. The number of individuals affected by Defendant's pixel tracking is expected to be massive, as Defendant serves nearly 3 million patients per year. Since most people use the internet to book appointments or view doctor profiles, the number of visits to the UC Health website which have been tracked via the unlawful pixels and tracking technology could be in the millions. The number of individuals who used Defendant's My Health Connection patient portal during the relevant period, and whose portal communications were tracked in the same manner, is substantial as well.

C. Defendant's Use of Tracking Pixels Violates HIPAA Standards

51. HIPAA and its implementing regulations protect individually identifiable health information and protected health information from unauthorized use and disclosure by covered entities, including healthcare providers such as Defendant.

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

53. "Individually identifiable health information" includes information, including demographic information collected from an individual, that is created or received by a health care provider, relates to the past, present, or future physical or mental health or condition of an individual or the provision of health care to an individual, and identifies the individual or provides a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. § 160.103.

54. Defendant is a covered entity under HIPAA because it is a healthcare provider that transmits health information in electronic form in connection with covered transactions.

55. Plaintiff does not allege merely that the disclosure of an IP address plus a visit to a generic unauthenticated webpage, standing alone, necessarily constitutes protected health information. Rather, Plaintiff alleges that Defendant disclosed user-submitted and user-selected healthcare communications from the Find a Doctor tool, including searches and selections concerning providers, specialties, symptoms, conditions, procedures, clinics, appointment-related information, insurance-related information, and locations, together with identifiers that could be used to identify the individual.

56. The information disclosed through Defendant's Tracking Pixel was created or received by Defendant, a healthcare provider; related to the provision of healthcare, medical treatment, symptoms, conditions, procedures, provider selection, and/or appointment-seeking activity; and identified Plaintiff and Class Members or provided a reasonable basis to identify them through IP addresses, device identifiers, cookie identifiers, browser identifiers, Facebook-linked identifiers, and/or other identifying information.

57. Defendant knowingly disclosed individually identifiable health information and protected health information to Meta/Facebook without Plaintiff's or Class Members' HIPAA-compliant authorization.

58. Defendant's disclosures to Meta/Facebook were not made for treatment, payment, or any valid health care operations that permitted disclosure of Plaintiff's and Class Members' protected health information to Meta/Facebook without authorization.

59. Defendant did not obtain Plaintiff's or Class Members' valid written HIPAA authorization to disclose their healthcare-related communications and identifying information to

Meta/Facebook for marketing, advertising, retargeting, analytics, patient-acquisition, or other commercial purposes.

60. Upon information and belief, Meta/Facebook was not acting as Defendant's business associate for the disclosures alleged herein, and Defendant did not have a valid business associate agreement authorizing Meta/Facebook to receive, maintain, use, or process Plaintiff's and Class Members' protected health information in compliance with HIPAA.

61. Even if Defendant contends that Meta/Facebook was providing analytics or advertising services to Defendant, Defendant was required to ensure that any disclosure of protected health information complied with HIPAA and was supported by a valid authorization, business associate agreement, or other lawful basis.

62. Defendant's unauthorized disclosure of Plaintiff's and Class Members' individually identifiable health information to Meta/Facebook violated HIPAA's standards for the protection of protected health information.

63. Defendant's conduct also violated 42 U.S.C. § 1320d-6 because Defendant knowingly disclosed individually identifiable health information to another person without authorization.

64. Defendant acted with intent to transfer and use individually identifiable health information for commercial advantage and personal gain because Defendant used the Tracking Pixel to improve marketing, analytics, advertising, retargeting, patient acquisition, and/or the efficiency and cost-effectiveness of its advertising campaigns.

65. Defendant's use of the Tracking Pixel caused precisely the privacy harms that HIPAA was designed to prevent: the unauthorized disclosure of sensitive healthcare-related communications and identifying information to third-party technology companies for non-

treatment purposes.

66. Accordingly, Defendant's use of the Tracking Pixel on the Find a Doctor tool violated HIPAA standards and supplies the criminal predicate that defeats any purported party-consent exception under the Electronic Communications Privacy Act.

D. Defendant Financially Benefitted From Its Use of the Pixel and the Unauthorized Disclosures at Issue.

67. The purpose and result of Defendant's use of the Tracking Pixel was marketing and profits.

68. Defendant's use of the Tracking Pixel permitted it to have access to enhanced advertising services and more cost-efficient marketing on its platforms.

69. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients using information collected by Facebook through the Tracking Pixel.

70. By utilizing the Tracking Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

E. Facts Specific to Plaintiff

71. Plaintiff Patrick Miller is a Colorado resident and patient of Defendant's healthcare network.

72. During the relevant period, Plaintiff used Defendant's Find a Doctor tool on Defendant's website to search for physicians, specialties, providers, clinics, symptoms, conditions, procedures, and/or treatment related to his healthcare needs.

73. Plaintiff is also a registered user of, and during the relevant period used, Defendant's My Health Connection patient portal to communicate with his healthcare providers

and access his personal health information, as well as book appointments to address certain health conditions.

74. Specifically, Plaintiff used Defendant's Find a Doctor tool to communicate healthcare-related information to Defendant, including searches and selections concerning specific medical providers, specialties, symptoms, conditions, procedures, treatment, location, insurance, and/or appointment-related information.

75. At the time Plaintiff used the Find a Doctor tool, Defendant had implemented and configured the Meta/Facebook Tracking Pixel on the tool. As a result, Plaintiff's healthcare-related communications with Defendant were contemporaneously duplicated, redirected, and transmitted to Meta/Facebook.

76. At the time Plaintiff used the My Health Connection patient portal, Defendant had, upon information and belief, implemented and configured the Meta/Facebook Tracking Pixel and/or similar tracking technology on the portal. As a result, upon information and belief, Plaintiff's healthcare-related communications with Defendant through the patient portal were contemporaneously duplicated, redirected, and transmitted to Meta/Facebook.

77. The information transmitted to Meta/Facebook included the substance of Plaintiff's healthcare-related communications with Defendant and was sent together with identifiers, including IP address, device identifiers, browser identifiers, cookie identifiers, Facebook-linked identifiers, and/or other information that could be used to connect the communication to Plaintiff. Upon information and belief, the same is true of the information Plaintiff transmitted to Defendant through the My Health Connection patient portal.

78. Plaintiff did not know of, consent to, agree to, authorize, or otherwise permit Defendant's interception, redirection, disclosure, or transmission of his healthcare-related

communications and identifying information to Meta/Facebook. This is true whether Plaintiff's communications were transmitted through the Find a Doctor tool or the My Health Connection patient portal.

79. As Defendant's patient, Plaintiff reasonably expected that his online communications with Defendant through the Find a Doctor tool were solely between himself and Defendant and would not be intercepted, duplicated, redirected, or transmitted to Meta/Facebook or any other unauthorized third party. Plaintiff's expectation of privacy was, if anything, heightened with respect to his communications through the My Health Connection patient portal, which required Plaintiff to log in with a secure username and password and which Defendant held out as a secure, confidential means of communicating with his healthcare providers.

TOLLING, CONCEALMENT, AND ESTOPPEL

80. The applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment and denial of the facts alleged herein given the affirmative representations and assurances of confidentiality featured in its Privacy Policy.

81. Defendant incorporated a Tracking Pixel into its Find a Doctor tool while providing users with no indication that their usage of the tool was being tracked and transmitted to third parties. Defendant knew that its Find a Doctor tool incorporated a Tracking Pixel yet it failed to disclose to Plaintiff and Class Members that their sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook. The same is true of Defendant's My Health Connection patient portal: Defendant provided no indication to patients that their use of the portal was being tracked and transmitted to third parties.

82. Plaintiff and the other Class Members could not with due diligence have discovered the full scope of Defendant's conduct, because there were no disclosures or other indication that

they were interacting with a website employing Facebook's Tracking Pixel technology that would disclose their Private Information.

83. All applicable statutes of limitation have also been tolled by operation of the discovery rule and the doctrine of continuing tort. Defendant's illegal interception and disclosure of Plaintiff's and the Class Members' Private Information have continued unabated through the present. What is more, Defendant was under a duty to disclose the nature and significance of its data collection practices but did not do so. Defendant is therefore estopped from relying on any statute of limitations defenses.

CLASS ALLEGATIONS

84. Plaintiff brings this class action on behalf of himself and on behalf of other similarly situated persons.

85. Plaintiff seeks to represent the following Class pursuant to Fed. R. Civ. P. 23:

> All individuals whose Private Information was disclosed by Defendant to Facebook without their authorization through its use of tracking pixels on its website and/or patient portal.

86. Excluded from the Class are: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, councils, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

87. The Class is so numerous that joinder of all members is impracticable. Upon information and belief, there are thousands of individuals whose Private Information may have been improperly used or disclosed by Defendant.

88. Class Members are readily identifiable from information in Defendant's possession.

89. There are questions of law and fact common to the Class that predominate over any questions affecting individual Class Members including:

a. Whether Defendant installed, configured, maintained, or used the Meta/Facebook Tracking Pixel on its Find a Doctor tool;

b. Whether Defendant installed, configured, maintained, or used the Meta/Facebook Tracking Pixel, or similar tracking technology, on its My Health Connection patient portal;

c. Whether Defendant's Tracking Pixel contemporaneously intercepted, redirected, duplicated, or transmitted communications between Plaintiff and Class Members and Defendant;

d. Whether the communications transmitted through Defendant's Find a Doctor tool constitute "electronic communications" under the Electronic Communications Privacy Act;

e. Whether the information transmitted to Meta/Facebook constituted the "contents" of Plaintiff's and Class Members' electronic communications;

f. Whether Defendant intentionally intercepted, disclosed, or used Plaintiff's and Class Members' electronic communications;

g. Whether Defendant procured Meta/Facebook to intercept Plaintiff's and Class Members' electronic communications;

h. Whether Plaintiff and Class Members consented to Defendant's interception, use, or disclosure of their electronic communications;

i. Whether Defendant's conduct was for the purpose of committing a criminal or tortious act, including the unauthorized disclosure of individually identifiable health information in violation of 42 U.S.C. § 1320d-6;

j. Whether Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*.;

k. Whether Plaintiff and Class Members are entitled to statutory damages, compensatory damages, punitive damages, equitable relief, declaratory relief, attorneys' fees, costs, and/or any other relief available under 18 U.S.C. § 2520; and

l. Whether class-wide injunctive and declaratory relief is appropriate.

90. 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 and incorporation of a Tracking Pixel on its Find a Doctor tool and patient portal.

91. 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 Plaintiff.

92. Plaintiff will fairly and adequately represent and protect the interests of the Class Members and Plaintiff has no conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff's injuries are typical of the other Class Members and Plaintiff has retained counsel experienced in complex class action litigation and intends to prosecute this action

vigorously.

93. Class treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein given the large number of Class Members and the relatively modest damages suffered by the Class Members who would otherwise not be able to afford to litigate their claims against Defendant.

94. Defendant's uniform conduct, the common claims shared amongst the Class Members, and the ascertainable identities of Class Members, demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

96. Defendant has acted or refused to act on grounds generally applicable to the Class as a whole by failing to notify Class Members of the disclosure of their Private Information through its use of a Tracking Pixel and to secure such information, and, accordingly, final injunctive or corresponding declaratory relief regarding the whole of the Class is appropriate.

COUNT I
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2510 *et seq.*
(On Behalf of Plaintiff and the Class)

97. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

98. The ECPA protects both the sending and receipt of electronic communications.

99. The ECPA provides a private right of action to any person whose wire, oral, or electronic communication is intercepted. 18 U.S.C. § 2520(a).

100. A violation of the ECPA occurs where any person/entity "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic communication" or "intentionally discloses, or endeavors to disclose, to any other

person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication" or "intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication." 18 U.S.C. §§ 2511(1)(a), (c)-(d).

101. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

102. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo opticalsystem that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

103. "Contents" includes "any information relating to the substance, purport, or meaning" of the communication at issue. 18 U.S.C. § 2510(8).

104. Plaintiff's and Class Members' interactions with Defendant's Find a Doctor tool were "electronic communications" under 18 U.S.C. § 2510(12) because they involved the transfer of signs, signals, writing, images, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce. The same is true of Plaintiff's and Class Members' interactions with Defendant's My Health Connection patient portal.

105. The information Plaintiff and Class Members communicated to Defendant through the Find a Doctor tool included the "contents" of their electronic communications under 18 U.S.C. § 2510(8) because it revealed the substance, purport, and meaning of their communications,

including searches and selections concerning providers, specialties, symptoms, conditions, procedures, treatment, clinics, appointment-related activity, insurance-related information, location, and other healthcare-related information. Upon information and belief, the same is true of information Plaintiff and Class Members communicated to Defendant through the My Health Connection patient portal.

106. Defendant intentionally installed, configured, maintained, and/or used the Meta/Facebook Tracking Pixel on the Find a Doctor tool and, on information and belief, its patient portal.

107. Defendant's Tracking Pixel constituted, or operated through, an electronic, mechanical, or other device under 18 U.S.C. § 2510(5), including code, scripts, cookies, browser instructions, and related tracking technology that caused Plaintiff's and Class Members' communications with Defendant to be contemporaneously duplicated, redirected, acquired, and transmitted to Meta/Facebook.

108. Whenever Plaintiff and Class Members interacted with Defendant's Find a Doctor tool, Defendant contemporaneously and intentionally intercepted, endeavored to intercept, and/or procured Meta/Facebook to intercept the contents of Plaintiff's and Class Members' electronic communications. The same is true, upon information and belief, whenever Plaintiff and Class Members interacted with Defendant's My Health Connection patient portal.

109. Defendant's interception occurred while Plaintiff's and Class Members' electronic communications were in transmission to Defendant because the Meta/Facebook Tracking Pixel caused those communications to be duplicated and transmitted to Meta/Facebook in real time or near real time.

110. Defendant intentionally disclosed, endeavored to disclose, used, and endeavored to

use the contents of Plaintiff's and Class Members' electronic communications while knowing or having reason to know that the information had been obtained through the interception of electronic communications.

111. Defendant disclosed the contents of Plaintiff's and Class Members' electronic communications to Meta/Facebook without Plaintiff's or Class Members' knowledge, consent, authorization, or valid written HIPAA authorization.

112. Plaintiff and Class Members did not intend to communicate with Meta/Facebook when using Defendant's Find a Doctor tool and did not consent to Defendant's interception, duplication, redirection, use, or disclosure of their communications to Meta/Facebook.

113. Defendant was a party to Plaintiff's and Class Members' communications with the Find a Doctor tool, but Defendant cannot invoke the party-consent exception under 18 U.S.C. § 2511(2)(d) because Defendant intercepted, used, and disclosed Plaintiff's and Class Members' communications for the purpose of committing criminal or tortious acts. Defendant was likewise a party to Plaintiff's and Class Members' communications made through the My Health Connection patient portal, and the same crime-tort analysis applies with equal force, because Defendant's interception and disclosure of information from the patient portal were, upon information and belief, made for the same unauthorized, HIPAA-violative purpose alleged above.

114. Specifically, Defendant intercepted, used, and disclosed Plaintiff's and Class Members' communications for the purpose of knowingly disclosing individually identifiable health information to Meta/Facebook without authorization in violation of 42 U.S.C. § 1320d-6.

115. Defendant's conduct violated 42 U.S.C. § 1320d-6 because Defendant knowingly disclosed individually identifiable health information to another person without Plaintiff's or Class Members' authorization.

116. Defendant acted with intent to transfer and use individually identifiable health information for commercial advantage and personal gain because Defendant used the Tracking Pixel and the resulting disclosures to improve marketing, advertising, analytics, retargeting, patient acquisition, website performance measurement, and/or the efficiency and cost-effectiveness of its marketing campaigns.

117. Defendant's disclosure of Plaintiff's and Class Members' healthcare-related communications and identifying information to Meta/Facebook was not necessary for treatment, payment, or any authorized healthcare purpose.

118. Defendant's disclosure of Plaintiff's and Class Members' healthcare-related communications and identifying information to Meta/Facebook was not supported by valid consent, valid HIPAA authorization, or any other lawful basis permitting the disclosure.

119. As a result, Defendant's interception, use, and disclosure of Plaintiff's and Class Members' communications falls outside the party-consent exception and violates 18 U.S.C. § 2511.

120. Defendant's conduct was intentional. Defendant chose to install, configure, maintain, and use the Tracking Pixel on the Find a Doctor tool, chose not to disable the Tracking Pixel on pages and tools that collected healthcare-related communications, and chose to benefit from the resulting transmissions to Meta/Facebook.

121. As a direct and proximate result of Defendant's violation of the ECPA, Plaintiff and Class Members suffered injury, including invasion of privacy, loss of control over their confidential healthcare communications and identifying information, disclosure of information they reasonably expected would remain private, diminution in the value of their private information, statutory damages, and other damages available by law.

122. As a direct and proximate result of Defendant's violation of the ECPA, Plaintiff and Class Members were damaged by Defendant's conduct in that:

a. Defendant harmed Plaintiff's and Class Members' interest in privacy;

b. Sensitive and confidential information that Plaintiff and Class Members intended to remain private has now been disclosed and is no longer private and confidential;

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

d. Defendant's actions diminished the value of Plaintiff's and Class Members' personal information.

123. As a result of Defendant's violations of the ECPA, Plaintiff and Class Members are entitled to all relief available under 18 U.S.C. § 2520, including preliminary, equitable, and declaratory relief; statutory damages of the greater of $100 per day for each day of violation or $10,000; compensatory damages; punitive damages in appropriate cases; and reasonable attorneys' fees and litigation costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Patrick Miller, Individually, and on behalf of all others similarly situated, prays for judgment as follows:

A. Certifying this action as a class action under Fed. R. Civ. P. 23, appointing Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Declaring that Defendant's conduct violated the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*;

C. Awarding Plaintiff and Class Members statutory damages, compensatory damages, and punitive damages as permitted under 18 U.S.C. § 2520;

D. Awarding appropriate preliminary, equitable, injunctive, and declaratory relief, including an order requiring Defendant to cease the unlawful interception, disclosure, and use of Plaintiff's and Class Members' electronic communications and private healthcare-related information;

E. Requiring Defendant to identify and disclose the categories of information intercepted, disclosed, transmitted, or otherwise made available to Meta/Facebook or any other unauthorized third party through the Tracking Pixel, including, without limitation, information intercepted, disclosed, or transmitted through Defendant's website (including the Find a Doctor tool) and Defendant's My Health Connection patient portal;

F. Awarding Plaintiff and Class Members reasonable attorneys' fees and litigation costs pursuant to 18 U.S.C. § 2520 and any other applicable law;

G. Awarding pre-judgment and post-judgment interest to the fullest extent permitted by law; and

H. Granting such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff, on behalf of himself, and all others similarly situated, hereby demands a trial by jury on all issues so triable.

Respectfully submitted,

PATRICK MILLER, individually and on behalf of similarly situated individuals

By: /s/ *Paul T. Geske*
One of Plaintiff's attorneys

Eugene Y. Turin
Paul T. Geske
Jordan R. Frysinger (*Admission Request Forthcoming*)
MCGUIRE LAW, P.C.
55 W. Wacker Drive, 9th Floor
Chicago, IL 60601
Tel: (312) 893-7002
Fax: (312) 275-7895
eturin@mcgpc.com
pgeske@mcgpc.com
jfrysinger@mcgpc.com

Counsel for Plaintiff and the putative Class Members