


OCT 25, 2023 02:29 PM



Ché Alexander, Clerk  
Fulton County Superior Court

IN THE SUPERIOR COURT OF FULTON COUNTY  
STATE OF GEORGIA

T.D., *individually*, and  
T.D., *on behalf of all others similarly  
situated*,

Plaintiff,

v.

PIEDMONT HEALTHCARE, INC.,

Defendant.

Case No.

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiff T.D. (“Plaintiff”),<sup>1</sup> a patient of Piedmont Healthcare, Inc. (“Piedmont” or “Defendant”), brings this class action lawsuit against PIEDMONT HEALTHCARE, INC. (“Piedmont” or “Defendant”) in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions, his counsel’s investigation and upon information and good faith belief as to all other matters, as follows:

**INTRODUCTION**

1. This class action lawsuit arises from Piedmont’s conscious decision to prioritize its desires for profit over its own responsibilities and its patients’ privacy rights. That is, and in order to gain greater insight into its patients’ purchasing decisions and habits, Piedmont embedded certain tracking technologies on its web properties to collect Plaintiff’s and Class Members’

---

<sup>1</sup> In order to avoid compounding the injuries and damages which give rise to this putative class action lawsuit and given the highly sensitive nature of the non-public, confidential and highly sensitive personal health information of Plaintiff disclosed by Defendant without permission, Plaintiff will move this Honorable Court for permission to proceed anonymously. *See, e.g., Doe v. Archdiocese of Atlanta*, 328 Ga. App. 324, n. 20, 761 S.E.2d 864, 869 (2014).

confidential and private medical information and then, in turn, to disclose it Meta Platforms, Inc., d/b/a Meta (“Facebook”).

2. Piedmont deployed this tracking technology to surreptitiously collect personally identifiable information (“PII”) and non-public protected health information (“PHI”)<sup>2</sup> including, but not limited to, demographic information such as email address, phone number, computer internet protocol (“IP”) address and contact information entered into Defendant’s web properties, and information such as appointment type and date, physician selected, button/menu selections and/or content, including PHI, typed into free text boxes on Defendant’s web properties without Plaintiff’s and Class Members’ knowledge or consent.

3. The Private Information of potentially millions of users of Defendant’s web properties was improperly and unlawfully disclosed to Facebook without their knowledge or consent.

4. Piedmont did so because it knew that this sensitive information had tremendous value and that Plaintiff and Class Members would *not* consent to the collection, disclosure and use of their Private Information in this manner.

5. Piedmont Healthcare is the largest healthcare provider in the State of Georgia, operating 23 hospitals, 65 urgent care centers and nearly 1,900 clinics in a state home to 11 million people.

6. Defendant disregarded the privacy rights of millions of visitors to and users of their websites by intentionally, willfully, recklessly and/or negligently failing to implement adequate and reasonable measures to ensure that that its users’ Private Information was safeguarded.

---

<sup>2</sup> This information is collectively referred to as “PII and PHI” or collectively, “Private Information.”

7. Instead, Defendant allowed unauthorized third parties, including Facebook, to intercept the users' clicks, communications on, and visits of Defendant's digital properties, including <https://www.piedmont.org/> (the "Website") and its "Piedmont MyChart" patient portal, available at [mychart.piedmont.org](https://mychart.piedmont.org) ("My Chart" or "Patient Portal") (collectively with the Website, the "Web Properties").

8. Prior to its collection and disclosure of Private Information to Facebook, Defendant encouraged and/or required Plaintiff and Class Members to use its digital properties, including MyChart, to receive healthcare services. Defendant's Website and Patient Portal encourage patients to provide Private Information as part of facilitating healthcare communications including, but not limited to, to search for a doctor, learn more about their conditions and treatments, access medical records and test results and make appointments.

9. At all times that Plaintiff and Class Members visited and utilized Defendant's Website and MyChart portal to receive medical services, they had a reasonable expectation of privacy that Private Information collected through Defendant's Web Properties and contained within the MyChart portal would remain secure and protected and only utilized for medical purposes.

10. Defendant further made expressed and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchange with Defendant.

11. The use of tracking technologies, such as the Facebook tracking pixel (the "Pixel") and related tracking technologies by Piedmont coincided with its executive leadership giving wide

reign to a new Chief Marketing Officer, Douwe Bergsma, who has heavily emphasized a focus on patient data and has viewed patients' adoption of digital tools as a key measure of success.<sup>3</sup>

12. Mr. Bergsma has stated: “[w]hether people book online, whether they check-in before they walk-in, whether they open a MyChart account, which is literally your account where all your data sits – and all of those metrics are also at a record high.”Mr. Bergsma continues “[t]hat was important because our campaign and our brand positioning was mostly about us being distinct in the marketplace, because we’d had this digital transformation at Piedmont that most healthcare systems haven't yet adopted – or at least to the same level ... Therefore, it was important that we measured them as well.”<sup>4</sup>

13. During this marketing campaign, Piedmont intentionally installed the Pixel on its Web Properties that secretly enabled the unauthorized transmission and disclosure of Plaintiff's and Class Members' confidential medical information.

14. On June 16, 2022, Piedmont was named in an article by The Markup regarding its use of the Meta Pixel to send Facebook highly sensitive health information that it collected from

---

<sup>3</sup> A pixel is a piece of code that “tracks the people and type of actions they take.” RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited Oct. 16, 2023). Pixels are routinely used to target specific customers by utilizing the data gathered through the pixel to build profiles for the purposes of retargeting and future marketing. Upon information and belief, Defendant utilized the Pixel data to improve and save costs on its marketing campaign, improve its data analytics, and attract new patients.

<sup>4</sup> *‘Almost overwhelmed’: How an ex-P&G US marketer ditched cohorts, personas, blended Ehrenberg-Bass, Binet & Field textbooks word for word, landed biggest marketing budget in \$7bn company’s history – and all KPIs are powering*, <https://www.mi-3.com.au/17-04-2023/how-ex-pg-us-marketer-ditched-cohorts-personas-and-restrictive-segmentation-blended-0> (last visited Oct. 16, 2023).

customers within the MyChart portal, which told Facebook the patient's name, the name of their doctor, and the time of their upcoming appointment.<sup>5</sup>

```
{"classList": "_Link+_actionable+_link+_readOnlyText+_InternalLink+m  
ain", "destination": "https://mychart.piedmont.org/PRD/app/communicat  
ion-center/conversation?id=ID REDACTED BY THE  
MARKUP", "id": "", "imageUrl": "/PRD/en-  
US/images/ProviderSilhouette.png", "innerText": "MyChart+Messaging+Us  
er\nREDACTED BY THE MARKUP\nAppointment+scheduled+from+MyChart\  
nThere+is+a+message+in+this+conversation+that+has+not+yet+been+view  
ed.\n 1 Appointment+For:+NAME REDACTED BY THE MARKUP+(ID REDACTED  
BY THE MARKUP)+Visit+Type:+NEW+PATIENT+(ID REDACTED BY THE MARKUP)+  
+ 2 MM/DD/YYYY+0:00+XX+00+mins.+ 3 NAME REDACTED BY THE  
MARKUP,+MD", "numChildButtons": 0, "tag": "a", "name": ""}
```

Source: mychart.piedmont.org, Mozilla Rally

15. Upon information and good faith belief, Piedmont had shared the sensitive healthcare information of millions of clients with an unauthorized third party, including Facebook, for years prior to the release of The Markup's article.

16. Operating as designed, Defendant's tracking Pixel allowed the Private Information that Plaintiff and Class Members submitted to Defendant to be unlawfully disclosed to Facebook.

17. For example, when Plaintiff or a Class Member accessed Defendant's Web Properties hosting the tracking Pixel, the Facebook software directed Plaintiff's or Class Members' browser to send a message to Facebook's servers. The information sent to Facebook by Defendant included the Private Information that Plaintiff and/or Class Members submitted to Defendant's Web Properties, including but not limited to, **the type and date of a medical appointment and**

---

<sup>5</sup> See <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> (last accessed October 24, 2023).

**physician.** Such Private Information would allow a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. This type of disclosure could also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy or AIDS.

18. Reiterating the importance of and necessity for data security and privacy concerning health information, the Federal Trade Commission (“FTC”) recently published a bulletin entitled *Protecting the privacy of health information: A Baker’s dozen takeaways from FTC cases*, in which it noted that:

[h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer’s health.*** Indeed, [recent FTC enforcement actions involving] *Premom, BetterHelp, GoodRx* and *Flo Health* ***make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or fertility, for example—or how they interact with that app (say, turning ‘pregnancy mode’ on or off) may itself be health information.***<sup>6</sup>

19. The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

**Don’t use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.**

In today’s surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use***

---

<sup>6</sup> See Elisa Jillison, *Protecting the privacy of health information: A Baker’s dozen takeaways from FTC cases*, the FTC Business Blog (July 25, 2023) (emphasis added), available at <https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases> (last visited Oct. 8, 2023).

consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.

[Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information.<sup>7</sup>

20. The exposed Private Information of Plaintiff and Class Members can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting or insurance companies utilizing the information to set insurance rates. Furthermore, third parties can often offer for sale the unencrypted, unredacted Private Information to criminals on the dark web for use in fraud and cyber-crimes.

21. Not only did Defendant willfully and intentionally incorporate the tracking Pixel into its Web Properties, but Defendant also never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications via the Web Properties with Facebook. As a result, Plaintiff and Class Members were unaware that their PII and PHI were being surreptitiously transmitted to Facebook as they communicated with their healthcare providers, looked up their conditions and/or treatments, and logged into the MyChart portal.

22. The full extent of Piedmont's unlawful disclosures is not yet known, but the numbers may be staggering. According to Piedmont's website, "Millions of patients conveniently engage with Piedmont online, *as they visited Piedmont.org and Piedmont MyChart over 30*

---

<sup>7</sup> *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization.

*million times, scheduled more than 515,000 online appointments and over 154,000 virtual visits.*”<sup>8</sup>

23. Defendant failed to issue a notice that Plaintiff’s and Class Members’ Private Information had been impermissibly disclosed to an unauthorized third party. In fact, Defendant never disclosed to Plaintiff or Class Members that they shared their sensitive and confidential communications, data, and Private Information with Facebook and other third parties.<sup>9</sup>

24. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiff’s and Class Members communications and medical information safe, secure, and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff’s and Class Members’ Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

25. Defendant, however, failed in its obligations and promises by utilizing the Facebook Pixel, described below, on its Web Properties knowing that such technology would transmit and share Plaintiff’s and Class Members’ Private Information with unauthorized third

---

<sup>8</sup> <https://www.piedmont.org/about-piedmont-healthcare/about-us-home> (emphasis added) (last accessed October 16, 2023).

<sup>9</sup> In contrast to Defendant, in recent months several healthcare providers which have installed the Meta Pixel on their Web Properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See, e.g., Cerebral, Inc. Notice of HIPAA Privacy Breach*, [https://cerebral.com/static/hippa\\_privacy\\_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf](https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf) (last accessed Oct. 24, 2023); Annie Burky, *Advocate Aurora says 3M patients’ health data possibly exposed through tracking technologies*, FIERCE HEALTHCARE (October 20, 2022), <https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3> (last accessed Oct. 25, 2023); *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWswire (August 19, 2022), <https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html>.



parties. Defendant breached its obligations and in one or more of the following ways: (i) failing to adequately review its marketing programs and web based technology to ensure the hospital Web Properties were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the 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 Members' Private Information through Facebook Pixels; (v) failing to warn Plaintiff and Class Members; and (vi) otherwise failing to design, and monitor its Web Properties in order to maintain the confidentiality and integrity of patient Private Information.

26. Plaintiff and Class Members have suffered injury because 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 unlawful disclosure of the Private Information, (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information, (v) statutory damages, and (v) the continued and ongoing risk to the Private Information.<sup>10</sup>

27. Plaintiff seeks to remedy these harms and bring causes of action for (1) Invasion of Privacy; (2) Breach of Fiduciary Duty; (3) Negligence; (4) Breach of Implied Contract; (5) Unjust Enrichment; (6) Breach of Confidence; (7) Bailment and (8) Violations of the Georgia Fair Business Practices Act, O.C.G.A. § 10-1-390, *et seq.*

## **PARTIES**

28. Plaintiff T.D. is a natural person and citizen of Georgia, residing in Decatur,

---

<sup>10</sup> It is unknown without discovery whether the Private Information was further disseminated to additional third-party marketing companies (*e.g.*, Google, Twitter, Bing, LinkedIn, HotJar, LifePerson, The Trade Desk, or Adobe) for the purposes of building profiles and retargeting or to insurance companies to set rates.

Georgia (DeKalb County), where he intends to remain.

29. Defendant Piedmont Healthcare, Inc. is a Georgia company with its principal place of business at 800 Howell Mill Road, Suite 850, Atlanta, GA, 30318. Defendant is a Georgia-wide integrated network of physician clinics, outpatient centers and hospitals. Its network consists of more than 23 hospitals, 12,000 doctors, 65 urgent care centers, and circa 1,900 clinics.

30. Headquartered in Atlanta, Georgia, Defendant advertises that it is committed to “empowering our patients through great care,” serving more than 3.7 million patients annually.

31. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 “HIPAA”)

#### **JURISDICTION & VENUE**

32. This Court has subject matter jurisdiction over this case under O.C.G.A. § 15-6-8.

33. This Court has personal jurisdiction over Defendant because it is organized under the laws of Georgia, transacts business in Georgia, and maintains its principal places of business in Georgia.

34. Venue is proper under O.C.G.A. § 9-10-93 because Fulton County was the county where a substantial part of the business was transacted, the tortious acts alleged herein occurred and the injury occurred.

#### **COMMON FACTUAL ALLEGATIONS**

##### ***A. Defendant Improperly Disclosed Plaintiff’s & Class Members’ Private Information***

35. In approximately 2020, Defendant launched a marketing campaign to connect Plaintiff and Class Members to Defendant’s digital healthcare platform with the goal of increasing revenue.

36. To accomplish this, Defendant utilized Facebook advertisements and intentionally installed the Pixel on its Web Properties. The Pixel is a piece of code that Defendant commonly used to measure activity and experiences on its Web Properties.

37. Through seeking and using Defendant's services as a medical provider, and utilizing the Web Properties services, including the My Chart portal, Plaintiff's and Class Members' Private Information was intercepted in real time and then disseminated to Facebook, and potentially to other third parties, via the Pixel that Defendant secretly installed on its Web Properties.

38. 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 movement and disclosing same to Facebook when they entered highly sensitive information on Defendant's Website and Patient Portal.

39. Defendant did not disclose to or warn Plaintiff or Class Members that Defendant used Plaintiff's and Class Members' Web Properties submissions for Facebook's marketing purposes.

40. Defendant tracked Plaintiff's and Class Members' Private Information via the Facebook Pixel from at least 2020 to approximately June 17, 2022.

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

42. Defendant's unauthorized disclosure is not just limited to activity on the public website, but the disclosure also involved information contained within the highly sensitive and private MyChart portal, which requires a specific login.

43. Upon information and belief, Defendant intercepted and disclosed the following

non-public private information to Facebook:

- a. Plaintiff's and Class Members' status as medical patients;
- b. Plaintiff's and Class Members' communications with Defendant through its Web Properties;
- c. Plaintiff's and Class Members' medical appointments, location of treatments, specific medical providers, and/or specific medical conditions and treatments; and
- d. Other sensitive and medical information contained within the MyChart portal.

44. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (i.e. Pixels) that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Facebook—an unauthorized third-party; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

***B. Operation Source Code***

45. Web browsers are software applications that allow consumers to exchange electronic communications over the internet.

46. Every website is hosted by a computer server through which the entity in charge of the website exchanges communications with Internet users via their web browsers.

47. The set of instructions that commands the browser is called the source code.

48. Source code may also command a web browser to send data transmissions to third parties via pixels or web bugs, tiny 1x1 invisible GIF files that effectively open a spying window through which a website funnels data about users and their actions to third parties.

49. The third parties to whom the website transmits data through pixels or web bugs do

not provide any substantive content relating to the user’s communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes.

50. The web bugs are tiny and camouflaged to purposefully remain invisible to the user.

51. Thus, without any knowledge, authorization, or action by a user, a website developer like Defendant can use its source code to commandeer the user’s computing device, causing the device to contemporaneously and invisibly re-direct the users personally identifiable non-public medical information to third parties.

**C. *The Facebook Pixel***

52. Defendant secretly deployed the Pixel on its Web Properties in violation of its common law, contractual, statutory, and regulatory duties and obligations.

53. The Facebook 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.”<sup>11</sup> It also allowed Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, learn about the website, and decrease advertising and marketing costs.<sup>12</sup>

54. Most importantly, it allowed Defendant and Facebook to secretly track patients on Defendant’s Web Properties and intercept their communications with the same.

**D. *Facebook’s Platform & its Business Tools***

55. Facebook operates the world’s largest social media company.

---

<sup>11</sup> <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last visited Oct. 16, 2023).

<sup>12</sup> *Id.*

56. In 2022, Facebook generated nearly \$117 billion in revenue.<sup>13</sup> Roughly 97% of that came from selling advertising space.<sup>14</sup>

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

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

59. Facebook then sells advertising space by highlighting its ability to target users.<sup>15</sup> Facebook can target users so effectively because it surveils user activity both on and off its site.<sup>16</sup> This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."<sup>17</sup> Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.<sup>18</sup>

---

<sup>13</sup> FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2022 RESULTS, <https://investor.fb.com/investor-news/press-release-details/2023/Meta-Reports-Fourth-Quarter-and-Full-Year-2022-Results/default.aspx> (last visited Oct. 16, 2023).

<sup>14</sup> *Id.*

<sup>15</sup> WHY ADVERTISE ON FACEBOOK, <https://www.facebook.com/business/help/205029060038706> (last visited Oct. 16, 2023).

<sup>16</sup> ABOUT FACEBOOK PIXEL, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last visited Oct. 16, 2023).

<sup>17</sup> AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting> (last visited Oct. 16, 2023).

<sup>18</sup> EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, <https://www.facebook.com/business/news/Core-Audiences> (last visited Oct. 16, 2023).

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

61. Advertisers can also build “Custom Audiences.”<sup>19</sup> Custom Audiences enable advertisers to reach “people who have already shown interest in [their] business, whether they’re loyal customers or people who have used [their] app or visited [their] website.”<sup>20</sup> With Custom Audiences, advertisers can target existing customers directly, and they can also build “Lookalike Audiences,” which “leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities.”<sup>21</sup> Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook’s “Business Tools.”<sup>22</sup>

62. As Facebook puts it, the Business Tools “help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook,

---

<sup>19</sup> ABOUT CUSTOM AUDIENCES, <https://www.facebook.com/business/help/744354708981227?id=2469097953376494> (last visited Oct. 16, 2023).

<sup>20</sup> AD TARGETING, *supra* note 15.

<sup>21</sup> About Lookalike Audiences, <https://www.facebook.com/business/help/164749007013531?id=401668390442328> (last visited Oct. 16, 2023).

<sup>22</sup> CREATE A CUSTOMER LIST CUSTOM AUDIENCE, <https://www.facebook.com/business/help/170456843145568?id=2469097953376494>; Facebook, Create a Website Custom Audience <https://www.facebook.com/business/help/1474662202748341?id=2469097953376494> (last visited Oct. 16, 2023).

understand and measure their products and services, and better reach and serve people who might be interested in their products and services.”<sup>23</sup> Put more succinctly, Facebook’s Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

63. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage’s Universal Resource Locator (“URL”) and metadata, or when a user downloads a mobile application or makes a purchase.<sup>24</sup> Facebook’s Business Tools can also track other events. Facebook offers a menu of “standard events” from which advertisers can choose, including what content a visitor views or purchases.<sup>25</sup> Advertisers can even create their own tracking parameters by building a “custom event.”<sup>26</sup>

64. One such Business Tool is the Facebook Pixel. Facebook offers this piece of code to advertisers, like Defendant, to integrate into their website. As the name implies, the Facebook

---

<sup>23</sup> THE FACEBOOK BUSINESS TOOLS, <https://www.facebook.com/help/331509497253087> (last visited Oct. 16, 2023).

<sup>24</sup> See FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, <https://developers.facebook.com/docs/facebook-pixel/advanced/>; see also FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>; FACEBOOK, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/> (last visited Oct. 16, 2023).

<sup>25</sup> SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>. (last visited Oct. 16, 2023).

<sup>26</sup> ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; see also FACEBOOK, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/>. (last visited Oct. 16, 2023),



Pixel “tracks the people and type of actions they take.”<sup>27</sup> When a user accesses a website hosting the Facebook Pixel, Facebook’s software script surreptitiously directs the user’s browser to send a separate message to Facebook’s servers. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser’s attempt to load and read Defendant’s websites—Defendant’s own code, and Facebook’s embedded code.

65. An example illustrates the point. Take an individual who navigates to Defendant’s website and clicks on a tab for “Diabetes.” When that tab is clicked, the individual’s browser sends a GET request to Defendant’s server requesting that server to load the particular webpage. Because Piedmont utilizes the Facebook Pixel, Facebook’s embedded code, written in JavaScript, sends secret instructions back to the individual’s browser, without alerting the individual that this is happening. Facebook causes the browser to secretly duplicate the communication with Piedmont, transmitting it to Facebook’s servers, alongside additional information that transcribes the communication’s content and the individual’s identity. Consequently, when Plaintiff and Class Members visited Defendant’s website and entered, e.g., Diabetes Management or Brain Tumor Treatment on Defendant’s Web Properties, their Private Information was transmitted to Facebook, including, but not limited to, their medical conditions and treatments sought, patient’s name, appointment type and date, physician selected, specific button/menu selections, and content typed into free text boxes. During the same transmissions, the Web Properties would also provide

---

<sup>27</sup> RETARGETING, *supra* note 2.

Facebook with the patient's unique personal identifiers including but not limited to their Facebook ID, IP address and/or device ID. This is precisely the type of information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.<sup>28</sup> Plaintiff's and Class Members' identities could 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.

66. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity. A user's Facebook Profile ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any other person—can use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

#### ***E. Defendant's Privacy Policies & Promises***

67. Defendant's privacy policies represent to Plaintiff and Class Members that Defendant will keep Private Information private and confidential, and it will only disclose Private Information under certain circumstances.

68. Defendant publishes several privacy policies that represent to patients and visitors to its Web Properties that Piedmont will keep sensitive information confidential and that it will

---

<sup>28</sup> See <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html> (last visited Oct. 16, 2023)

only disclose PII and PHI provided to it under certain circumstances, none of which apply here.<sup>29</sup>

69. Defendant's separate Notice of Privacy Practices assures Plaintiff and Class Members that Piedmont is "committed to keeping your health information private."<sup>30</sup>

70. Defendant's Notice of Privacy Practices explains Defendant's legal duties with respect to PHI and the exceptions for when Defendant can lawfully use and disclose Plaintiff's and Class Members' PHI in the following ways:

- For Treatment;
- For Payment;
- For Health Care Operations;
- For Medical Research;
- As Required by Law and Law Enforcement;
- For Public Health Activity;
- For Health Oversight Activities;
- Organ, Eye and Tissue Donation;
- Coroners, Medical Examiners, Funeral Directors and  
Individuals Involved in Your Health Care or Payment for  
Your Health Care;
- Uses and Disclosures for Involvement in Your Care;
- To Avoid a Serious Threat to Health or Safety or in

---

<sup>29</sup> <https://www.piedmont.org/about-piedmont-healthcare/joint-notice/privacy-policy> (last accessed Oct. 16, 2023).

<sup>30</sup> <https://www.piedmont.org/media/file/PHC-Joint-Notice-Privacy-Practice.pdf> (last accessed Oct. 16, 2023).

Disaster Relief Efforts;

- Specialized Government Functions;
- Workers' Compensation;
- Fundraising Efforts;
- Appointment Reminders, Follow-Up Care and Treatment

Alternatives;

- Patient Directories.<sup>31</sup>

71. Defendant also promises patients that, "Other types of uses and disclosures of your PHI not described in this Notice will be made only with your written authorization."<sup>32</sup>

72. Defendant's privacy policy does not permit Defendant to use and disclose Plaintiff's and Class Members' Private Information for marketing purposes.

73. Defendant violated its own privacy policy by unlawfully intercepting and disclosing Plaintiff's and Class Members' Private Information to Facebook and third parties without adequately disclosing that it shared Private Information with third parties and without acquiring the specific patients' consent or authorization to share the Private Information.

***F. Defendant Violated HIPAA Standards***

74. 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.<sup>33</sup>

---

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

<sup>33</sup> HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

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

76. In *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, the Department instructs:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data... If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.<sup>34</sup>

77. In its guidance on Marketing, the Department further instructs:

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, ***covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.***<sup>35</sup>

### **G. Defendant Violated Industry Standards**

78. A medical provider's duty of confidentiality is embedded in the physician-patient

---

<sup>34</sup>

[https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/De-identification/hhs\\_deid\\_guidance.pdf](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/De-identification/hhs_deid_guidance.pdf) (last visited Oct. 16, 2023)

<sup>35</sup><https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/marketing.pdf> (emphasis added) (last visited Oct. 16, 2023).

and hospital-patient relationship, it is a cardinal rule.

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

80. 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)

81. 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.

82. 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.

***H. Plaintiff's & Class Members' Expectations of Privacy***

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

84. Indeed, at all times when Plaintiff and Class Members provided their PII and PHI

to Defendant, they each had a reasonable expectation that the information would remain private and that Defendant would not share their Private Information with third parties for a commercial purpose, unrelated to patient care.

***I. IP Addresses are Personally Identifiable Information***

85. Through the use of the Pixel, computer IP addresses are among the Private Information that was improperly disclosed to Facebook.

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

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

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

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

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

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

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

- a. HIPAA defines personally identifiable information to include “any unique identifying number, characteristic or code” and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).
  - b. HIPAA further declares information as personally identifiable where the covered entity has “actual knowledge that the information to identify an individual who is a subject of the information.” 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. § 164.514(b)(2)(i)(O).
93. Consequently, by disclosing Plaintiff’s and Class Members’ IP addresses,

Defendant's business practices violated HIPAA and industry privacy standards.

***J. Defendant was Enriched and Benefitted from the Use of The Pixel & Unauthorized Disclosures.***

94. The sole purpose of the use of the Facebook Pixel on Defendant's Web Properties was marketing and revenue.

95. 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.

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

97. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients connected to the Piedmont MyChart portal.

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

**REPRESENTATIVE PLAINTIFF'S EXPERIENCES**

99. Plaintiff T.D. entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff T.D. disclosed his Private Information to Defendant.

100. On numerous occasions, from 2016 to present, Plaintiff T.D. accessed mychart.piedmont.org and Defendant's Website on his mobile device and/or computer to receive healthcare services from Defendant and at Defendant's direction.

101. Plaintiff T.D. used Defendant's Web Properties to look for health care providers and to schedule doctor's appointments for himself.



102. For example, in October 2021 Plaintiff T.D. used Defendant's MyChart to make a doctor's appointment that he attended in November 2021.

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

104. Plaintiff T.D. provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

105. Plaintiff T.D. reasonably expected that his communications with Defendant via the Web Properties were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

106. Pursuant to the systematic process described herein, Piedmont assisted Facebook with intercepting Plaintiff T.D.'s communications, including those that contained personally identifiable information, protected health information, and related confidential information.

107. Defendant transmitted to Facebook Plaintiff T.D.'s Facebook ID, computer IP address; and information such as his medical conditions, treatments sought, appointment type and date, and physician selected.

108. Piedmont assisted these interceptions without Plaintiff T.D.'s knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff T.D.'s personally identifiable information and protected health information.

109. Defendant did not inform Plaintiff T.D. that it had shared his Private Information with Facebook.

110. Plaintiff T.D. is diagnosed with a specific medical condition and submitted information to Defendant's website about scheduling medical appointments for his medical

condition to Facebook.

111. Plaintiff T.D. suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of his Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (v) the continued and ongoing risk to his Private Information.

112. Plaintiff T.D. has a continuing interest in ensuring that Plaintiff T.D.'s Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future unauthorized disclosure.

#### **TOLLING**

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

114. The Meta Pixel and other tracking tools on Defendant's Web Properties were and are entirely invisible to a Web Properties visitor.

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

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

117. Defendant had exclusive knowledge that its Web Properties incorporated the Meta Pixel and other tracking tools and yet failed to disclose to its patients, including Plaintiff and Class Members, that by seeking medical care through Defendant's Website, Plaintiff's and Class Members' Private Information would be disclosed or released to Facebook and other unauthorized third parties.

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

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

120. 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.

#### **CLASS ACTION ALLEGATIONS**

121. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class") pursuant to O.C.G.A. § 9-11-23.

122. The Class that Plaintiff seeks to represent is defined as follows:

All Georgia citizens whose Private Information was disclosed to a third party without authorization or consent through the Pixel on Defendant's Web Properties.

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

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

125. **Numerosity, O.C.G.A. § 9-11-23(a)(1)**: The Class members are so numerous that

joinder of all members is impracticable. Upon information and belief, there are millions of individuals whose PII and PHI may have been improperly accessed by Facebook, and the Class is identifiable within Defendant's records.

126. **Commonality, O.C.G.A. § 9-11-23(a)(2) and (b)(3)**: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect 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; and
- l. 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.

127. **Typicality, O.C.G.A. § 9-11-23(a)(3)**: Plaintiff's claims are typical of those of

other Class Members because all had their PII and PHI compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

128. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully disclosed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. 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.

129. **Adequacy of Representation, O.C.G.A. § 9-11-23(a)(4)**: Plaintiff will fairly and adequately represent and protect the interests of the 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.

130. **Superiority and Manageability, O.C.G.A. § 9-11-23(b)(3)**: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require.

Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

131. **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 Plaintiff.

132. 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 they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which 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.

133. 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.

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

135. 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.

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

137. 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 policy;
- 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;
- 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.

## **CLAIMS FOR RELIEF**

### **COUNT I**

#### **INVASION OF PRIVACY - INTRUSION UPON SECLUSION *(On Behalf of Plaintiff & the Class)***

138. 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 Class.

139. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

140. Defendant owed a duty to Plaintiff and Class Members to keep their PII and PHI confidential.

141. The unauthorized disclosure and/or acquisition by a third party of Plaintiff's and Class Members' PII and PHI is highly offensive to a reasonable person.

142. Defendant's willful and intentional disclosure of Plaintiff's and Class Members' PII and PHI constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind



that would be highly offensive to a reasonable person.

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

144. Defendant failed to protect Plaintiff's and Class Members' Private Information and acted with a knowing state of mind when it incorporated the Facebook Pixel into its website because it knew the functionality and purpose of the Facebook Pixel.

145. Because Defendant intentionally and willfully incorporated the Facebook Pixel into its Web Properties and encouraged patients to use those Web Properties for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff and Class Members.

146. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiff and the Class Members was disclosed to a third party without authorization, causing Plaintiff and the Class to suffer damages.

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

148. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII and PHI are still maintained by Defendant and still in the possession of Facebook and the wrongful disclosure of the information cannot be undone.

149. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A

judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook, who on information and belief continues to possess and utilize that information.

150. Plaintiff, on behalf of himself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII and PHI and to adhere to its common law, contractual, statutory, and regulatory duties.

## **COUNT II**

### **BREACH OF FIDUCIARY DUTY** **(On Behalf of Plaintiff & the Class)**

151. 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 Class.

152. In light of the special relationship between Defendant Piedmont and Plaintiff and Class Members, whereby Defendant Piedmont 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 Piedmont did and does store.

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

154. Defendant Piedmont 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.

155. As a direct and proximate result of Defendant Piedmont'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 III**

#### **NEGLIGENCE**

#### **(On Behalf of Plaintiff & the Class)**

156. 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 Class.

157. Defendant Piedmont required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare services.

158. Upon accepting, storing, and controlling the Private Information of Plaintiff and the Class in its computer systems, Defendant owed, and continues to owe, a duty to Plaintiff and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information from disclosure to third parties.

159. Defendant breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

160. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' Private Information through its use of the Pixels and other tracking technologies would result in unauthorized third parties, such as Facebook, gaining access to such Private Information for no lawful purpose.

161. Defendant's duty of care to use reasonable measures to secure and safeguard

Plaintiff's and Class Members' Private Information arose due to the special relationship that existed between Defendant and its patients, which is recognized by statute, regulations, and the common law.

162. In addition, Defendant had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

163. Defendant Piedmont's duty to use reasonable security measures under HIPAA required Defendant Piedmont 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.

164. In addition, Defendant Piedmont 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.

165. Defendant Piedmont'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.

166. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and

Class Members and their Private Information.

167. Defendant's misconduct included the failure to (1) secure Plaintiff's and Class Members' Private Information; (2) comply with industry standard data security practices; (3) implement adequate website and event monitoring; (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Pixels and other tracking technologies; and (5) prevent unauthorized access to Plaintiff's and Class Members' Private Information by sharing that information with Facebook and other third parties. Defendant's failures and breaches of these duties constituted negligence.

168. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and Class members' Private Information, Plaintiff and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

169. Defendant's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiff's and Class members' Private Information constituted (and continue to constitute) negligence at common law.

170. Plaintiff and Class Members are entitled to compensatory, nominal, and/or punitive damages, and Plaintiff and Class Members are entitled to recover those damages in an amount to be determined at trial.

171. Defendant Piedmont'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 Piedmont to (i)

strengthen its data security systems and monitoring procedures; (ii) cease sharing Plaintiff's and Class Members' Private Information with Facebook and other third parties without Plaintiff's and Class Members' express consent; and (iii) submit to future annual audits of its security systems and monitoring procedures.

#### **COUNT IV**

##### **BREACH OF IMPLIED CONTRACT (On behalf of Plaintiff & the Class)**

172. 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 Class.

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

174. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

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

176. Defendant Piedmont breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information to a third party, *i.e.*, Facebook.

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

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

**COUNT V**

**UNJUST ENRICHMENT**  
***(On behalf of Plaintiff and the Class)***

179. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein—with the express exception of Plaintiff's Breach of Implied Contract count—and brings this claim individually and on behalf of the proposed Class.

180. This count is pled in the alternative to Plaintiff's Breach of Implied Contract count.

181. Defendant Piedmont benefits from Plaintiff and Class Members and unjustly retained those benefits at their expense.

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

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

184. The benefits that Defendant Piedmont derived from Plaintiff and Class Members were not offered by Plaintiff and Class Member gratuitously and rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in Georgia for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the

unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

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

## **COUNT VI**

### **BREACH OF CONFIDENCE *(On behalf of Plaintiff and the Class)***

186. 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 Class.

187. In Georgia, medical providers have a duty to their patients to keep non-public medical information completely confidential.

188. Plaintiff had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's website and on the log-in page for Defendant's MyChart portal.

189. Plaintiff's reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its privacy policy.

190. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant Piedmont deployed pixel code to disclose and transmit Plaintiff's personally identifiable, non-public medical information, and the contents of their communications exchanged with Defendant to third parties.

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

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



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

194. 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 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.

195. As a result, Plaintiff and Class Members are entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation.

## **COUNT VII**

### **BAILMENT**

#### ***(On Behalf of Plaintiff & the Class)***

196. 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 Class.

197. Defendant acquired and was obligated to safeguard the Private Information of Plaintiff and Class Members.

198. Defendant accepted possession and took control of Plaintiff's and Class Members' Private Information under such circumstances that the law imposes an obligation to safeguard the property of another.

199. Specifically, a constructive bailment arises when Defendant, as is the case here, takes lawful possession of the property of another and has a duty to account for that property, without intending to appropriate it.

200. Constructive bailments do not require an express assumption of duties and may arise from the bare fact of the thing coming into the actual possession and control of a person fortuitously, or by mistake as to the duty or ability of the recipient to effect the purpose contemplated by the absolute owner.

201. During the bailment, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care, diligence and prudence in protecting their Private Information.

202. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class Members' Private Information, resulting in the unlawful and unauthorized access to and misuse of such Private Information.

203. Defendant further breached its duty to safeguard Plaintiff's and Class Members' Private Information by failing to notify them that their Private Information had been disclosed without patient authorization and compromised.

204. As a direct and proximate result of Defendant's breach of duty, Plaintiff and Class Members have suffered compensable damages that were reasonably foreseeable to Defendant, including but not limited to, the damages set forth herein.

### **COUNT VIII**

#### **VIOLATIONS OF THE GEORGIA FAIR BUSINESS PRACTICES ACT**

##### **O.C.G.A. § 10-1-390, *et seq.* (On Behalf of Plaintiff & the 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 Class.

206. Georgia's Fair Business Practices Act, O.C.G.A. § 10-1-390, prohibits deceptive acts or practices in the conduct of any business, trade, or commerce in the state of Georgia.

207. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the O.C.G.A. § 10-1-390(a) and (b). The conduct alleged herein took place in the context of the consumer marketplace.

208. Defendant stored Plaintiff's and Class Members' Private Information in Defendant's electronic databases. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with all relevant regulations and would have kept Plaintiff's and Class Members' Private Information secure and prevented the loss or misuse of that Private Information. Defendant did not disclose to Plaintiff and Class Members that its data systems were not secure.

209. Plaintiff and Class Members would not have provided their Private Information if they had been told or knew that Defendant failed to maintain sufficient security thereof, and its inability to safely store Plaintiff's and Class Members' Private Information.

210. As alleged herein in this Complaint, Defendant engaged in the unfair or deceptive acts or practices in the conduct of consumer transactions in violation of O.C.G.A. § 10-1-390, including but not limited to:

- Unlawfully disclosing Plaintiff's and Class Members' Private Information to Facebook and other third parties;
- Failing to disclose or omitting material facts to Plaintiff and Class Members regarding the disclosure of their Private Information to Facebook and other third parties;
- Failing to take proper action to ensure the Pixel was configured to prevent unlawful disclosure of Plaintiff's and Class Members' Private Information;
- Representing that its services were of a particular standard or quality that Defendant knew or should have known were of another;
- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the disclosure of that Private Information to third parties, including Facebook;
- Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the disclosure to third parties, including Facebook;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;
- Omitting, suppressing, and concealing the material fact that Defendant did not reasonably or adequately secure Plaintiff's

and Class Members' Private Information; and

- Omitting, suppressing, and concealing the material fact that Defendant did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by HIPAA, which was a direct and proximate cause of the disclosure of that Private Information to third parties, including Facebook.

211. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant knew it failed to disclose to Plaintiff and Class Members that their healthcare related communications via the Web Properties would be disclosed to Facebook and other third parties.

212. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability—or willingness—to protect the confidentiality of consumers' Private Information.

213. Defendant's actions also constitute deceptive and unfair acts or practices because Defendant intended that Plaintiff and Class Members rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

214. Specifically, Defendant was aware that Plaintiff and Class Members depended and relied upon it to keep their communications with their healthcare providers confidential, and Defendant instead disclosed that information to Facebook.

215. In addition, Defendant's material failure to disclose that Defendant collects Plaintiff's and Class Members' Private Information for marketing purposes with Facebook constitutes an unfair act or practice prohibited by O.C.G.A. § 10-1-390. Defendant's actions were immoral, unethical, and unscrupulous.

216. Plaintiff and Class members had reasonable expectations of privacy in their

communications exchanged with Defendant, including communications exchanged at mychart.piedmont.org and on their MyChart portal.

217. 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 Notice of Privacy Practices.

218. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed pixel code to disclose and transmit Plaintiff's and Class Members' personally identifiable, non-public medical information, and the contents of their communications exchanged with Defendant to third parties, i.e., Facebook.

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

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

221. Such acts by Defendant are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her Private Information to Defendant. Said deceptive acts and practices are material. The requests for and use of such Private Information in Georgia through deceptive means occurring in Georgia were consumer acts or practices and thereby fall under Georgia's Fair Business Practices Act, O.C.G.A. § 10-1-390.

222. In addition, Defendant's failure to secure patients' Private Information violated HIPAA and therefore violates O.C.G.A. § 10-1-390.

223. The aforesaid conduct violated O.C.G.A. § 10-1-390, in that it is a restraint on trade or commerce.

224. Defendant's violations of O.C.G.A. § 10-1-390 has an impact and general importance to the public, including the people of Georgia. Millions of residents of Georgia have had their Private Information stored on Defendant's Web Properties, many of whom have been impacted by the unlawful disclosure of PHI to Facebook and other third parties.

225. As a direct and proximate result of these deceptive trade practices, Plaintiff and Class Members are entitled to judgment under O.C.G.A. § 10-1-390, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

226. On information and belief, Defendant formulated and conceived of the systems used to compile and maintain patient information largely within the state of Georgia, oversaw its data privacy program complained of herein from Georgia, and its communications and other efforts to hold patient data largely emanated from Georgia.

227. Most, if not all, of the alleged misrepresentations and omissions by Defendant that led to inadequate measures to protect patient information occurred within or were approved within Georgia.

228. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and Class Members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the services were of another, inferior quality), in violation of O.C.G.A. § 10-1-390.

229. Accordingly, Plaintiff, on behalf of himself and Class Members, brings this action under O.C.G.A. § 10-1-390 to seek such injunctive relief necessary to enjoin further violations and recover costs of this action, including reasonable attorneys' fees and other costs.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Class and appointing Plaintiff and their Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;
- C. For 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. For an award of damages, including, but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.



**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands that this matter be tried before a jury.

Date: October 25, 2023

Respectfully Submitted,

**PEIFFER WOLF CARR  
KANE CONWAY & WISE, LLP**

By: /s/ Andrew R. Tate

Andrew R. Tate

GA Bar # 518068

235 Peachtree St. NE, Suite 400

Atlanta, GA 30303

Ph: 404-282-4806

atate@peifferwolf.com

Brandon M. Wise

IL Bar # 6319580\*

One US Bank Plaza, Suite 1950

St. Louis, MO 63101

Ph: (314) 833-4825

bwise@peifferwolf.com

**ALMEIDA LAW GROUP LLC**

David S. Almeida

NY Bar # 3056520\*

Elena Belov

NY Bar # 4080891\*

Britany Kabakov

IL Bar # 6336126\*

849 W. Webster Avenue

Chicago, Illinois 60614

Ph: (312) 576-3024

david@almeidlawgroup.com

elena@almeidlawgroup.com

britany@almeidlawgroup.com

*\*pro hac vice* admission to be sought

*COUNSEL FOR PLAINTIFF  
& THE CLASS*

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Piedmont Healthcare Facing Class Action Over Alleged Sharing of User Data with Facebook](#)

---