

**IN THE CIRCUIT COURT OF THE SEVENTEENTH JUDICIAL CIRCUIT,
IN AND FOR BROWARD COUNTY, FLORIDA**

**KENNETH KOSKOSKY, VICTORIA
WITHERBY, and SANDRA HOOVER** on
behalf of themselves and all others similarly
situated,

Plaintiffs,

v.

DAVITA, INC.

Defendant.

Civil Action No.

DEMAND FOR A JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiffs Kenneth Koskosky, Victoria Witherby, and Sandra Hoover (“Plaintiffs”) bring this Class action complaint (“Complaint”) on behalf of themselves, and all other similarly situated patients (the “Class Members”) against DaVita Inc., (“DaVita”), which operates, controls, and manages dialysis centers throughout the country, including in the state of Florida. Defendant owns and controls DaVita.com (the “Website”), affiliate patient portals, and a mobile application that’s available for download (collectively the “Online Platforms”). The allegations contained in this Class Action complaint, which are based on Plaintiffs’ knowledge of facts pertaining to themselves and their own actions and counsels’ investigations, and upon information and belief as to all other matters, are as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action lawsuit to address DaVita’s use of tracking technologies on its Online Platforms, which divulged patients’ personally identifiable information (“PII”) and protected health information (“PHI”) (collectively referred to as “Private Information”)

CLASS ACTION COMPLAINT

to unauthorized third parties, including Meta Platforms, Inc. d/b/a Meta (“Facebook” or “Meta”) and Google LLC (“Google”).

2. The tracking tools at issues include the Facebook Pixel, Facebook SDK, Facebook Conversions API, Google Analytics, Google Tag Manager, DoubleClick (owned by Google), and all related tools (collectively, “Tracking Technologies”).¹

3. These Tracking Technologies allowed unauthorized third parties to intercept and receive the contents of patients’ communications and Private Information when they used the Online Platforms.

4. DaVita encouraged its patients to use the Web Properties in conjunction with their medical care, and in doing so, knew or should have known patients would use the Online Platforms to communicate Private Information.

5. Plaintiffs and other Class Members who used DaVita’s Online Platforms reasonably believed they were communicating only with their trusted healthcare provider, and nothing about the Online Platforms’ appearance indicated that unauthorized third parties could intercept and obtain Private Information submitted by patients.

6. Unbeknownst to Plaintiffs and Class Members, however, DaVita’s Online Platforms contained Tracking Technologies within their source code that surreptitiously track and transmit Plaintiffs’ and Class Members’ online activity and communications (including intimate details about their medical treatment and appointments) to third parties without first obtaining their permission, in violation of HIPAA, state laws, industry standards, and patient expectations.

¹ This Complaint contains images and evidence demonstrating the Facebook Pixel was used on the Online Platforms until June of 2023, but Plaintiffs do not know every tracking and/or marketing tool that was previously installed on the Online Platforms during the relevant period, when they first began using DaVita’s Online Platforms.

7. For example, DaVita used the Facebook Pixel, which “tracks the people and [the] type of actions they take”² in real time as they interact with a website, including the exact text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), among other things.

8. The Pixel allowed the Private Information that Plaintiffs and Class Members submitted to Defendant to be unlawfully disclosed to Facebook alongside their unique and persistent Facebook ID (“FID”), IP address, and other static identifiers.

9. By installing and using Tracking Technologies on its Online Platforms, DaVita effectively planted a bug on Plaintiffs’ and Class Members’ web browsers that caused their communications to be intercepted, accessed, viewed, and captured by third parties in real time based on DaVita’s chosen parameters.

10. The Office for Civil Rights at HHS has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates (“regulated entities”) under the HIPAA Privacy, Security, and Breach Notification Rules (“HIPAA Rules”) when using online tracking technologies (“tracking technologies”), such as the Tracking Technologies.³ The Bulletin expressly provides (in bold type) that “[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.” In other words, HHS has expressly stated that DaVita’s implementation of Tracking Technologies violates HIPAA Rules.

² See, e.g., Facebook, *Retargeting*, https://www.facebook.com/business/goals/retargeting_ (last visited Oct. 20, 2023)(explaining how the pixel tracks and transmits website users’ interactions and communications, allowing for individualized retargeting and marketing).

³ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH & HUMAN SERV., <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited Oct. 20, 2023).

11. The information DaVita divulged to unauthorized third-parties allowed those entities to learn that specific individuals were patients seeking and receiving treatment at DaVita's dialysis medical centers.

12. In and of itself, this reveals the fact that an individual is being treated for kidney disease and has received or will receive dialysis services and adjacent services to treat that particular medical condition. In turn, this information was used and/or sold to additional unauthorized parties for use in marketing and geotargeting.

13. Patients simply do not anticipate that their trusted healthcare provider will send their personal health information or confidential medical and health information to social media and marketing companies for future exploitation and targeted marketing. Neither Plaintiffs nor any other Class Member signed a written authorization permitting DaVita to send their Private Information to Facebook. Similarly, DaVita does not have a HIPAA-compliant Business Associate Agreement in place with Meta or Google.

14. Consequently, Plaintiffs bring this action for legal and equitable remedies to address and rectify the illegal conduct and actions described herein, to enjoin DaVita from making similar disclosure of its patients' Private Information in the future, and to fully articulate, *inter alia*, the specific Private Information it disclosed to third parties and to identify the recipients of that information.

15. As a result of DaVita's conduct, Plaintiffs and Class Members have suffered numerous injuries, including invasion of privacy, loss of benefit of the bargain, diminution of value of the Private Information, statutory damages, and the continued and ongoing risk to their Private Information.

16. Plaintiffs seek to remedy these harms and brings causes of action for (1) violations of Cal. Penal Code § 630, *et seq.*; (2) violations of Cal. Civ. Code § 56, *et seq.*; (3) violations of Cal. Bus. & Prof. Code § 17200, *et seq.*; (4) Violation of the Florida Security of Communications Act, Florida Statutes § 934.01, *et seq.*; (5) intrusion upon seclusion; (6) publication of private facts; and (7) breach of confidence.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action seeking declaratory relief, injunctive relief, and damages in excess of \$50,000.00 (exclusive of court costs, attorney's fees, and interest), pursuant to Article V, section 5(b), of the Florida Constitution and Florida statutes §§ 26.012 and 86.011.

18. This Court has personal jurisdiction over DaVita because it regularly conducts business, maintains several facilities, and treats patients in Broward County, Florida.

19. Venue is proper under Florida Statutes §§ 47.011, *et seq.*, because many of the privacy violations alleged herein occurred in Broward County, Florida.

THE PARTIES

20. Plaintiff Kenneth Koskosky is an adult citizen of the State of Florida and was a patient of DaVita from 2017 through 2022. He used DaVita's Online Platforms in conjunction with and in order to obtain the medical treatment and services he received from Defendant beginning in 2017.

21. Plaintiff Victoria Witherby is a California resident who has been a patient of DaVita for several years and started using its Online Platforms in or around 2022.

22. Plaintiff Sandra Hoover is a California resident who has been a patient of DaVita for several years and started using its Online Platforms in or around 2022.

CLASS ACTION COMPLAINT

23. DaVita, Inc. is headquartered in Colorado and owns 236 medical clinics and dialysis treatment centers in Florida, including facilities in Broward county. According to its website, DaVita is a kidney dialysis specialist health care organization that develops solutions that will transform healthcare for patients with kidney disease, provides integrated care to help people better manage their kidney disease, and conducts clinical trial services across the spectrum of pharmaceutical and medical device development.⁴

FACTUAL ALLEGATIONS

A. Background

24. Facebook operates the world's largest social media company and generated \$117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.⁵

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

26. Facebook's Business Tools, including the 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 website visitors' activity.

27. One such Business Tool is the Pixel, which "tracks the people and type of actions they take."⁶ When a user accesses a webpage hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers.

⁴ <https://www.DaVita.com/about> (last visited April 25, 2023).

⁵ Facebook, *Meta Reports Fourth Quarter and Full Year 2021 Results*, FACEBOOK, <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited April 25, 2023).

⁶ FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting>. (Last visited April 25, 2023).

Notably, this transmission does not occur unless the webpage contains the Pixel. Stated differently, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook but for the Defendant's decisions to install the Pixel on its webpage(s).

28. As explained in more detail below, this secret transmission to Facebook is initiated by Defendant's source code concurrently with Plaintiffs' and Class Members' communications to their intended recipient, Defendant.

B. DaVita Assisted Third Parties in Intercepting Patients' Communications with its Online Platforms and Disclosed Plaintiffs' and Class Members' Private Information to Third Parties.

29. Defendant's Online Platforms are accessible on mobile devices and desktop computers and allow patients to communicate with Defendant regarding the patients' past, present, and future health or medical care, as well as their past, present, and future medical bills and payments.

30. DaVita encouraged patients to use the Online Platforms to communicate their private medical information, schedule appointments and facility tours, access information about their treatments, pay medical bills, view test results, and more.

31. Despite this, DaVita purposely installed Tracking Technologies on its Online Platforms and programmed specific webpage(s) to surreptitiously share its patients' private and protected communications, including Plaintiffs' and Class Members' PHI and PII, which was sent to Facebook, Google, and additional third parties.

32. The Tracking Technologies followed, recorded, and disseminated patients' information as they navigated and communicated with DaVita via the Online Platforms, simultaneously transmitting the substance of those communications to unintended third parties.

33. The information disseminated by the Tracking Technologies and/or intercepted by third parties constitutes Private Information, including medical information patients requested or viewed, the title of any buttons they clicked (such as the “Request Treatment” button, which indicates the patients has requested treatment), the exact phrases users typed into text boxes (e.g., “symptoms of kidney disease”), selections they made from drop-down menus or while using filtering tools (such as “In-Center Hemodialysis,” which indicates the exact treatment and therapy the user is seeking and also reveals their medical symptoms and conditions), and other sensitive and confidential information, the divulgence of which is and was highly offensive to Plaintiffs.

34. As described by the HHS Bulletin, this is protected health information (PHI) because “the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual’s past, present, or future health or health care or payment for care.”

35. The information collected and disclosed by DaVita’s Tracking Tools is not anonymous and is viewed and categorized by the intercepting party on receipt.

36. The information Facebook received via the Tracking Tools was linked and connected to patients’ Facebook profiles (via their Facebook ID or “c_user id”), which includes other identifying information.

37. Similarly, Google “stores users’ logged-in identifier on non-Google website in its logs. Whenever a user logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the user’s browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses these data for serving personalized ads.”

38. Simply put, the health information that was disclosed via the Tracking Tools is personally identifiable and was sent alongside other persistent identifiers such as the patients' IP address, Facebook ID, and device identifiers.^{7,8}

39. As described by the HHS Bulletin, this is protected health information (PHI) even if the visitor has no previous relationship with DaVita because "the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care."⁹

i. **DaVita's Tracking Technologies, Source Code, Interception of HTTP Requests and Transmission of HTTP Requests.**

40. Web browsers are software applications that allow consumers to navigate the internet and exchange electronic communications, and every "client device" (computer, tablet, or smart phone) has a web browser (e.g., Microsoft Edge, Google Chrome, Mozilla's Firefox browser, etc.).

41. Correspondingly, every website is hosted by a computer "server" which allows the website's owner (Defendant) to display the Website and exchange communications with the website's visitors (Plaintiffs and Class Members) via the visitors' web browser.

⁷ See *Brown v. Google, Inc.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049 (N.D. Cal. 2021) (citing internal evidence from Google employees). Google also connects user data to IP addresses; IP addresses have been classified by the United States Department of Health and Human Services ("HHS") as personally identifying information. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dept of Health and Hum. Servs. (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

⁸ <https://developers.facebook.com/docs/meta-pixel/> (last accessed May 5, 2023).

⁹ See HHS Bulletin § *How do the HIPAA Rules apply to regulated entities' use of tracking technologies?*

42. When patients used the Online Platforms, they engaged in an ongoing back-and-forth exchange of electronic communications with DaVita wherein their web browser communicated with DaVita's computer server—similar to how two telephones would communicate.

43. These communications are invisible to ordinary consumers¹⁰, but one browsing session may consist of thousands of individual HTTP Requests and HTTP Responses.

44. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as a "Find a Dialysis Center" page), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Webpage(s)).

45. Every webpage is comprised of both Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

46. DaVita's Tracking Technologies were embedded in its Online Platforms' Source Code, which is contained in its HTTP Response. The Tracking Technologies, which were programmed to automatically track patients' communications and transmit them to third parties, executed instructions that effectively opened a hidden spying window into each patients' web browser, through which third parties intercepted patients' communications and activity while using DaVita's Online Platforms.

¹⁰ See HHS Bulletin § *What is a tracking technology?* ("Tracking technologies collect information and track users in various ways, many of which are not apparent to the website or mobile app user.").

47. For example, when a patient visits www.DaVita.com and selects the “Find a Dialysis Center” button, the patient’s browser automatically sends an HTTP Request to Defendant’s web server. Defendant’s web server automatically returns an HTTP Response, which loads the Markup for that webpage. As depicted below, the user only sees the Markup, not Defendant’s Source Code or underlying HTTP Requests and Responses.

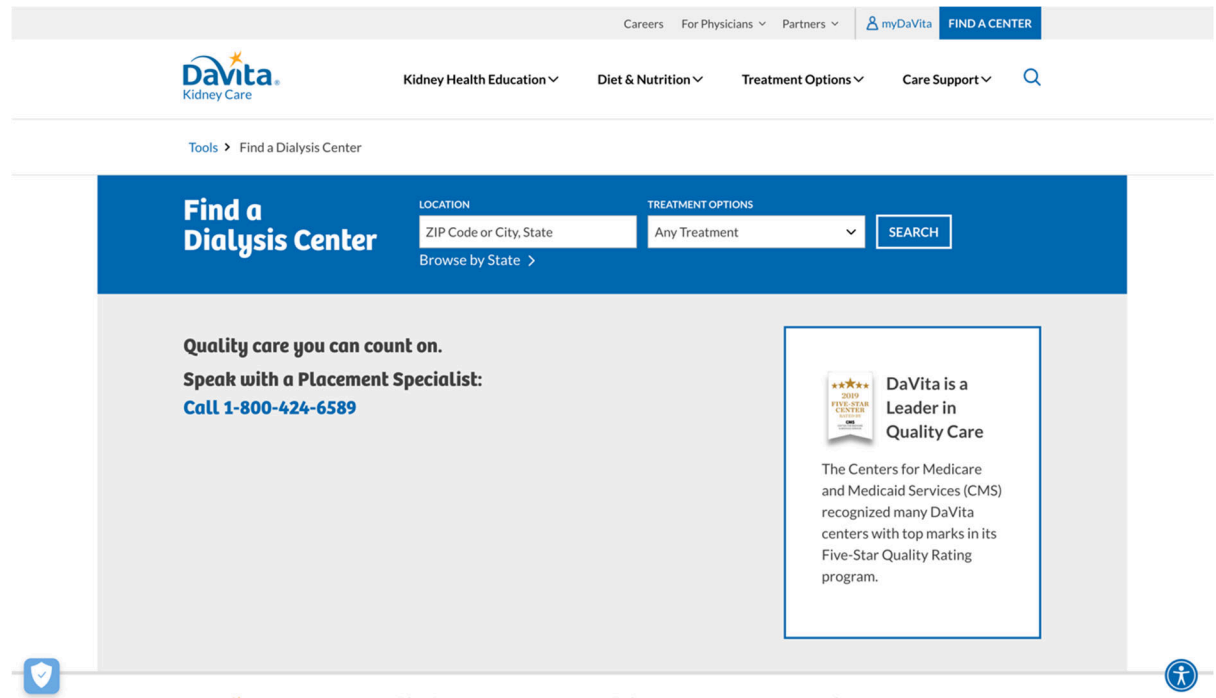


Figure 1. The image above is a screenshot taken from the user’s web browser upon visiting <https://www.DaVita.com/tools/find-dialysis-center?> (Last accessed Apr. 25, 2023).

48. The patient visiting this webpage only sees the Markup, not Defendant’s Source Code or underlying HTTP Requests and Responses.

49. Accordingly, DaVita’s Source Code manipulated its patients’ web browsers by secretly instructing them to duplicate the communications (HTTP Requests) and send them to third parties contemporaneously, invisibly, and without its patients’ knowledge.

50. Thus, without its patients' consent, Defendant has effectively used its source code to commandeer and "bug" or "tap" patients' computing devices, allowing Facebook and other third parties to listen in on all their communications and intercept their Private Information.

51. Consequently, when Plaintiffs and Class Members visited the Online Platforms and communicated their Private Information—such as their specific dialysis treatment or therapy, use of online tools, payment portals, and access to medical records—their confidential communications were simultaneously intercepted and transmitted.

C. DaVita Disclosed Plaintiffs' and Class Members' Private Information to Facebook Using the Pixel and/or Conversions API Tracking Technologies.

52. DaVita utilized Facebook's Business Tools and intentionally installed the Pixel, SDK, and Conversions API on its Online Properties, and this is evidence by DaVita's unique Facebook identifier (represented as "id=1922159211337179"; "id=802325101033656"; "id=530586864070598 and/or "id=825898851225030") that can be used to identify which of its webpages contain the Pixel.

53. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences (for future targeting marketing and advertising), and decrease its advertising and marketing costs. However, Defendant's Website does not require the Pixel to function.

54. Plaintiffs and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to Facebook, nor did they intend for Facebook to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

55. Defendant's Pixel and Conversions API sent non-public Private Information to Facebook, including but not limited to information about Plaintiffs' and Class Members' past, present, or future health or health care, such as their: (1) status as medical patients; (2) health conditions; (3) location information; (4) online payment activities; and (5) web searches.

56. Importantly, the Private Information was to Facebook sent alongside Plaintiffs' and Class Members' IP address and Facebook ID (c_user cookie or "FID"), thereby linking an individual patient's Private Information to their unique Facebook accounts, real identity, and any other information in Facebook's possession.¹¹ Because a Facebook ID uniquely identifies an individual's account, Facebook—or any ordinary person—can easily use it to locate, access, and view the corresponding profile.

57. If a user accessed Defendant's Website while they were logged into Facebook, such as in the examples above, their c_user cookie—which contains the user's unencrypted FID—was transmitted to Facebook alongside 6 other cookies:

Name	Value	Domain
sb	EviWYHBCNlrLUD...	.facebook.com
c_user	100001028527210	.facebook.com
usida	eyJ2ZXliOjEslmlkljo...	.facebook.com
datr	LUNgZOg84ndHb...	.facebook.com
m_ls	%7B%22c%22%3...	.www.facebook.com
xs	21%3Ak8h4z26wK...	.facebook.com
fr	0x8LFPnGedeb4iic...	.facebook.com

¹¹ Defendant's Website tracks and transmits data via first-party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

58. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies.

Name	Value	Domain
sb	EviWYHBCNlrLUD...	.facebook.com
usida	eyJ2ZXliOjEslmlkljo...	.facebook.com
datr	LUNgZOg84ndHb...	.facebook.com
m_ls	%7B%22c%22%3...	.www.facebook.com
dpr	2	.facebook.com
fr	0ZqcFQtTjwegi5tq...	.facebook.com

59. If a visitor has never created an account, an even smaller set of cookies are transmitted.

fr	0ZqcFQtTjwegi5tq...	.facebook.com
----	---------------------	---------------

60. At each stage, Defendant also utilizes the `_fbp` cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user.¹²

<code>_fbp</code>	fb.1.168235772...	.davita.com
-------------------	-------------------	-------------

61. The Pixel uses both first- and third-party cookies, and both were used on the Website.¹³

¹² *Id.*

¹³ A first-party cookie is “created by the website the user is visiting”—in this case, Defendant’s Website. A third-party cookie is “created by a website with a domain name other than the one the user is currently visiting”—i.e., Facebook. The `_fbp` cookie is always transmitted as a first-party cookie. At a minimum, Facebook uses the `fr`, `_fbp`, and `c_user` cookies to link website visitors’ data to their Facebook IDs and corresponding accounts.

i. **Defendant’s Tracking Technologies Disseminate Patient Information Entered on the Online Platforms**

62. An example illustrates the point. If a patient uses www.DaVita.com to request a dialysis treatment, Defendant’s Website directs the patient to communicate Private Information, including their dialysis service, last time they received treatment, treatment frequency, their date of birth, their contact information, their street address, and their insurance provider. Unbeknownst to the patient, every communication is sent to Facebook, including the medical condition the patient types into the search bar and the filters they select.

63. In the example below, the user searched for a dialysis facility that offers “Home Hemodialysis” and is located near their address, of “70 Hahnemann Lane, Napa, CA 94558, USA”.

Find a Dialysis Center

LOCATION: 70 hahnemann Ln Napa
Browse by State >

TREATMENT OPTIONS: Home Hemodialysis

SEARCH

3 total results for 70 Hahnemann Ln, Napa, CA 94558

1 DaVita Fairfield At Home 13.48 MILES AWAY

No Rating Available
4660 Central Way
Fairfield, CA 94534-1803
[Get Directions](#)

Treatment Options:
Home Hemo
Phone: **1-800-424-6589**
Fax: 707-863-7384
Reference Number: 6201

REQUEST TREATMENT **SCHEDULE A TOUR**

2 DaVita Curtola Ht At Home 17.35 MILES AWAY

No Rating Available
125 Corporate Pl, Ste B

Treatment Options:
Home Hemo

REQUEST TREATMENT

Speak with a Placement Specialist
Call 1-800-424-6589

Map showing location near Napa, CA.

64. Unbeknownst to ordinary patients, this webpage—which is undoubtedly used to communicate Private Information for the purpose of seeking medical treatment—contains Tracking Technologies.

65. The image below shows the “behind the scenes” portion of the website that is invisible to ordinary users, and each row of text in the right column represents just one instance in which Facebook received the communications made via the website.

The screenshot displays a web browser interface with two patient profiles and a network traffic analysis tool. The first profile, 'eld At', is located at 70 Hahnemann Ln, Napa, CA 94558, 13.48 miles away. The second profile, 'la Ht At', is located at 17.35 miles away. Both profiles show treatment options: Home Hemo, Phone: 1-800-424-6589, Fax: 707-863-7384, and Reference Number: 6201. The network traffic panel shows a list of requests, with the selected request displaying a long query string containing various parameters and tracking identifiers.

70 Hahnemann Ln, Napa, CA 94558

eld At 13.48 MILES AWAY

Treatment Options:
Home Hemo
Phone: 1-800-424-6589
Fax: 707-863-7384
Reference Number: 6201

REQUEST TREATMENT

SCHEDULE A TOUR

la Ht At 17.35 MILES AWAY

Treatment Options:
Home Hemo
Phone: 1-800-424-6589
Fax: 707-642-1349

Network Traffic Panel:

Name	Headers	Payload	Preview	Response	Initiator	Timing	Cookies
gtm.js?id=GTM-KHKQMM8							
optimize.js?id=GTM-NK59N25							
js?id=DC-4189903							
js?id=DC-12833848							
js?id=G-P0206SNQ2G&l=da...							
px?id=1157732&seg=19156...							
px?id=1220731&seg=20958...							
px?id=1103239&seg=17634...							
px?id=1119999&seg=18071...							
?id=1800808309967269&ev...							
?id=1922159211337179&ev...							
?id=802325101033656&ev...							
?id=530586864070598&ev...							
?id=825898851225030&ev...							
?id=1922159211337179&ev...							
?id=802325101033656&ev...							
?id=1922159211337179&ev...							
?id=802325101033656&ev...							
https://www.facebook.com/t/7...							
https://www.facebook.com/t/7...							

66. Thus, without alerting the user, every communication was sent to Facebook as they used the Website, and the screenshot below shows what Private Information was sent when patients used the Website to “Requested Treatment.”

```
× Headers Payload Preview Response Initiator Timing Cookies
▼ Query String Parameters view source view URL-encoded
id: 1922159211337179
ev: SubscribedButtonClick
dl: https://www.davita.com/tools/find-dialysis-center?location=70%20hahnemann%20Ln%20Napa&lat=38.337473&
rl: https://www.davita.com/
if: false
ts: 1682544039186
cd[buttonFeatures]: {"classList":"btn no-scroll","destination":"https://www.davita.com/tools/find-dialysis-center?location=70%20hahnemann%20Ln%20Napa&lat=38.337473&...",
cd[buttonText]: REQUEST TREATMENT
cd[formFeatures]: []
cd[pageFeatures]: {"title":"Find a Dialysis Center | Tools | DaVita Kidney Care"}
sw: 1680
sh: 1050
v: 2.9.102
r: stable
ec: 2
o: 2078
cs_est: true
fbp: fb.1.1682357722564.1074487812
it: 1682543336772
coo: false
es: automatic
tm: 3
rqm: GET
```

67. The first line of highlighted text, “id: 1922159211337179,” refers to DaVita’s Pixel ID and confirms that it implemented the Pixel into its Source Code for this webpage and transmitted info to Facebook from this webpage.

68. The second line of text, “ev: SubscribedButtonClick,” identifies and categorizes which actions the user undertook (“ev:” refers to event, and “SubscribedButtonClick” is the type of event). Thus, this identifies the patient as having viewed the specific webpage after

communicating their search criteria, and it also identifies them as having clicked the button titled “[innertext]: REQUEST TREATMENT.”.

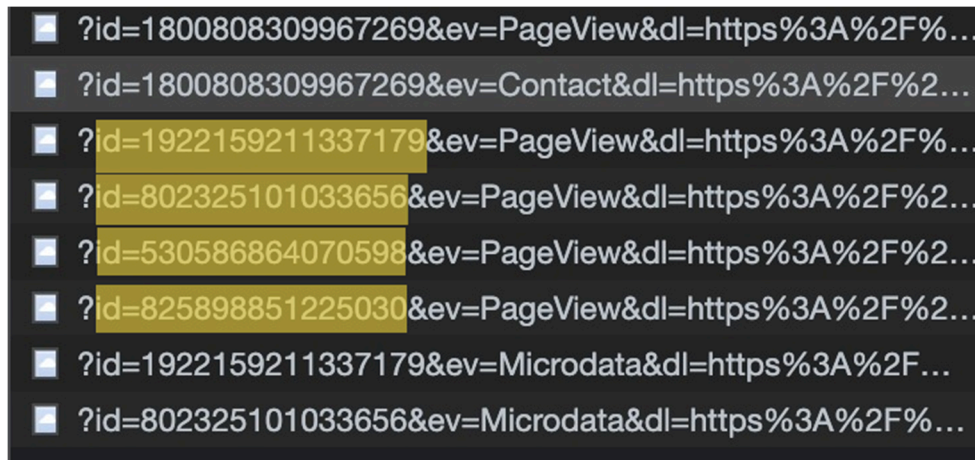
69. The next lines of highlighted text show Defendant disclosed to Facebook: (1) the fact that the user is a patient or prospective patient seeking medical care from Defendant via www.DaVita.com (“request treatment”); (2) the requested treatment or therapy; (3) the user’s address (“location=70 Hahnemann Ln. Napa”); and (4) the city of the treatment center provided.

70. Finally, the highlighted text (“GET”) combined with the user’s Facebook ID (highlighted as “c_user=” in the image below) demonstrates that Facebook received the Private Information alongside the user’s Facebook ID (c_user ID), thereby linking it to their specific Facebook profile.¹⁴

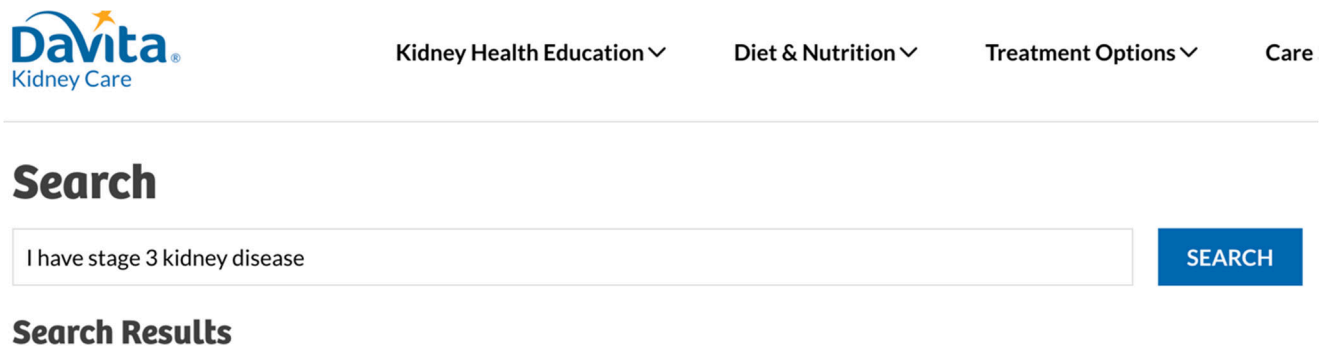
```
▼ Request Headers
:authority: www.facebook.com
:method: GET
:path: /tr/?id=1922159211337179&ev=Microdata&dl=https%3A%2F%2Fwww.davita.com%2Ftools%2Ffind-dialysis-center%2Frequest-treatment%2Fca%2Ffairfield%2F4660-central-way--6201&rl=https%3A%2F%2Fwww.davita.com%2Ftools%2Ffind-dialysis-center%3Flocation%3D70%2520hahnemann%2520Ln%2520Napa%26lat%3D38.337473%26lng%3D-122.327802%26modalities%3D3%26p%3D1&if=false&ts=1682544041568&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22Request%20Treatment%22%2C%22meta%3Adescription%22%3A%22%2C%22meta%3Akeywords%22%3A%22%2C%22%7D&cd[OpenGraph]=%7B%22og%3Aurl%22%3A%22https%3A%2F%2Fwww.davita.com%2Ftools%2Ffind-dialysis-center%2Frequest-treatment%2Fca%2Ffairfield%2F4660-central-way--6201%22%2C%22og%3Atype%22%3A%22website%22%2C%22og%3Atitle%22%3A%22Request%20Treatment%22%2C%22og%3Adescription%22%3A%22%2C%22og%3Aimage%22%3A%22https%3A%2F%2Fwww.davita.com%2F%2Fmedia%2Fdavita%2Fproject%2Fcommon%2Flogo%2Fdavita_dkc_logo_rgb_f_72dpi.png%22%2C%22twitter%3Aimage%22%3A%22https%3A%2F%2Fwww.davita.com%2F%2Fmedia%2Fdavita%2Fproject%2Fcommon%2Flogo%2Fdavita_dkc_logo_rgb_f_72dpi.png%22%7D&cd[Schema.org]=%5B%5D&cd[JSON-LD]=%5B%5D&sw=1680&sh=1050&v=2.9.102&sr=stable&sec=1&o=30&fbp=fb.1.1682357722564.10744878126&it=16825440404176&coo=fal
se&es=automatic&tm=3&rqm=GET
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
cookie: sb=EviWYHBCNlrLUDYEWueWfxSg; datr=EviWYDgxK3-uisplR2ui9347; dpr=2; locale=en_US; c_user=1; m_ls=%7B%22c%22%3A%7B%7D%2C%22d%22%3A%22fc345b4a-bf6d-4a6a-bee7-98714caee2db%22%2C%22s%22%3A%221%22%2C%22u%22%3A%227juehv%22%7D; usida=eyJ2ZXIiOiJEsImkIjoiQXJ0cDM1Y2ozcWZxYiIsInRpbWUiOiJlE20DI0NjYyMzV9"; xs=21%3Ak8h4z26wKtSPlw%3A2%3A1682458251%3A-1%3A2699%3A%3AAcXM7AFnEg6mXErwVjoTewBMsAugmbzmW6vT7yhflLw; fr=0jDAUD0Y98paof0px.AWWTiu2MXZJefw9u-iYtWZ6ys88.BkSZV6.ks.AAA.0.0.BkSZV6.AWXdze5ZTI4
referer: https://www.davita.com/tools/find-dialysis-center/request-treatment/ca/fairfield/4660-central-way--6201
sec-ch-ua: "Google Chrome";v="111", "Not(A:Brand";v="8", "Chromium";v="111"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
sec-fetch-dest: image
```

¹⁴ The user’s Facebook ID is represented as the c_user ID highlight in the image above, and Plaintiff has redacted the corresponding string of numbers to preserve the user’s anonymity.

71. As seen in the image below, one singular communication was sent to Facebook four times via four distinct pixel ids.

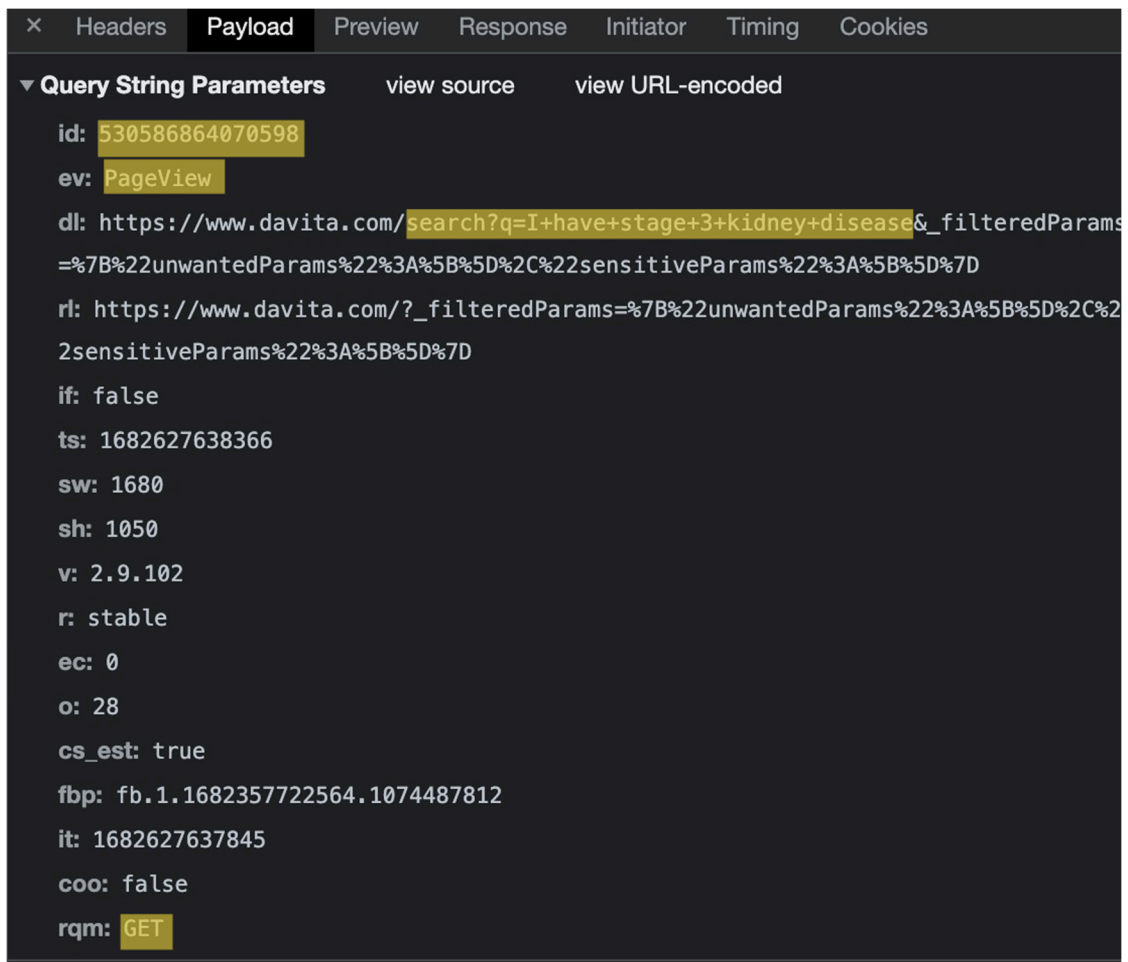


72. Defendant also disseminated and/or allowed the interception of its patients' exact search terms and phrases as they typed them in search bars.



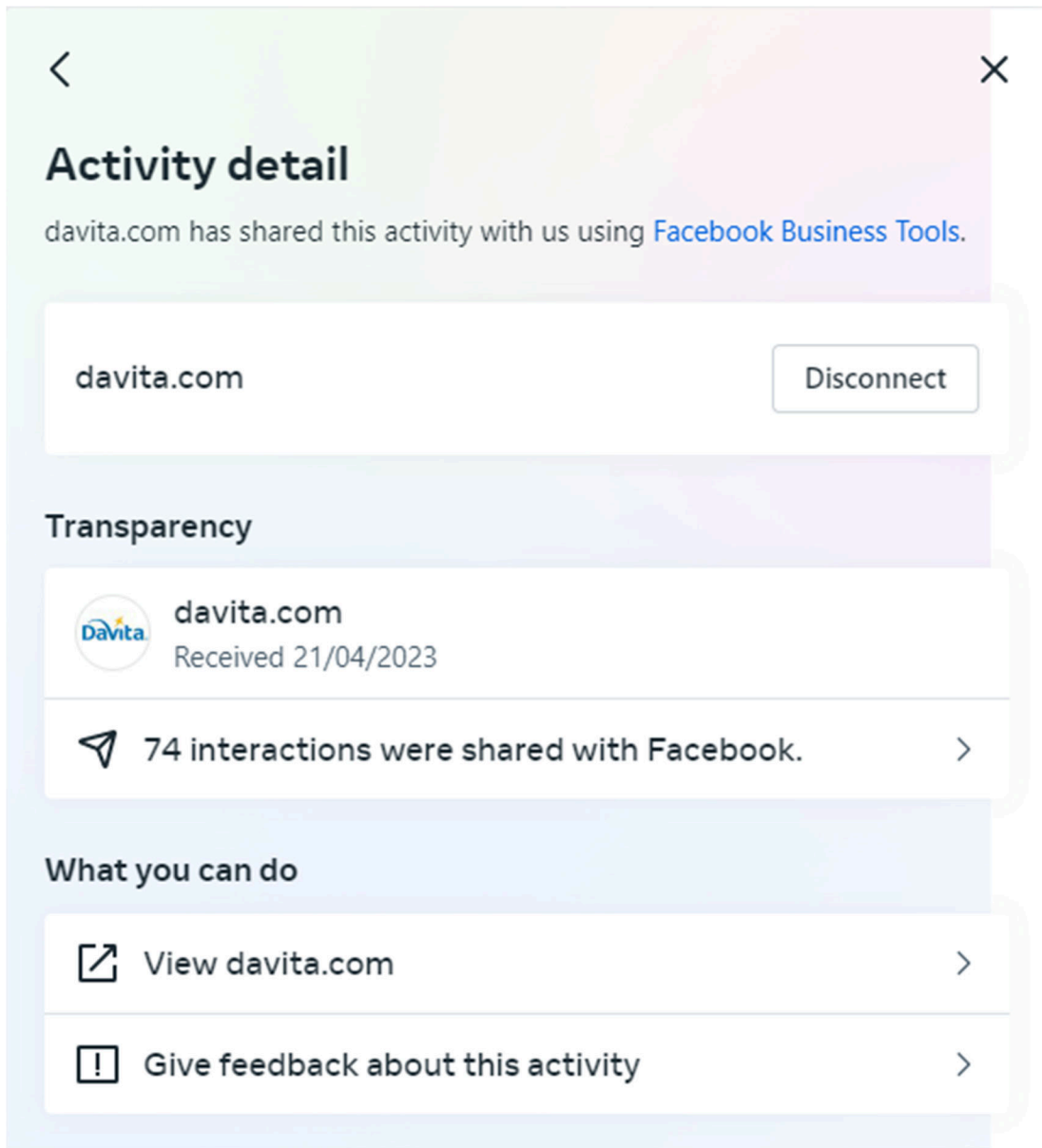
73. If a patient typed "I have stage 3 kidney disease" into the search bar and pressed "search," the exact phrase was received by Facebook, thereby revealing their PHI.

74. In turn, that PHI was viewed and used by Facebook, linked to their individual Facebook account, and used for marketing and advertising.




```
× Headers Payload Preview Response Initiator Timing Cookies
▼ Request Headers
:authority: www.facebook.com
:method: GET
:path: /tr/?id=530586864070598&ev=PageView&dl=https%3A%2F%2Fwww.davita.com%2Fsearch%3Fq%3DI%2Bhave%2Bstage%2B%2
Bkidney%2Bdisease%26_filteredParams%3D%257B%2522unwantedParams%2522%253A%255B%255D%252C%2522sensitiveParams%252
2%253A%255B%255D%257D&rl=https%3A%2F%2Fwww.davita.com%2F%3F_filteredParams%3D%257B%2522unwantedParams%2522%253
A%255B%255D%252C%2522sensitiveParams%2522%253A%255B%255D%257D&if=false&ts=1682627638366&sw=1680&sh=1050&v=2.9.1
02&r=stable&ec=0&o=28&cs_est=true&fbp=fb.1.1682357722564.1074487812&it=1682627637845&coo=false&rqm=GET
:scheme: https
accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
:cookie: sb=EviWYHBCnlrLUDYEWueWfxSg; datr=EviWYDgxK3-uisplr2ui9347; dpr=2; locale=en_US; c_user=1
0; m_ls=%7B%22c%22%3A%7B%7D%2C%22d%22%3A%22fc345b4a-bf6d-4a6a-bee7-98714caee2db%22%2C%22s%22%3A%221%22%2C%22u%2
2%3A%227juehv%22%7D; usida=eyJ2ZXIiOiJEsImklIjojIjoiQXJ0cDM1Y2ozcWZxYiIsInRpbWUiOiJlE2ODI0NjYyYmZV9; xs=21%3Ak8h4z26wKt
SPlw%3A2%3A1682458251%3A-1%3A2699%3A%3AAcW0Hw02thceJP9AXxDvTmWFhsNBmH9ojRC4nHovs7E; fr=0tnjoJqiyJDI096wr.AWXNtd
E5kU1Qc-Uf6u1KifXY6yE.BkStuH.ks.AAA.0.0.BkStuH.AWXAIn6hFHg
:referer: https://www.davita.com/search?q=I%20have%20stage%20%20kidney%20disease
sec-ch-ua: "Google Chrome";v="111", "Not(A:Brand";v="8", "Chromium";v="111"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
sec-fetch-dest: image
sec-fetch-mode: no-cors
sec-fetch-site: cross-site
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.
0.0 Safari/537.36
```

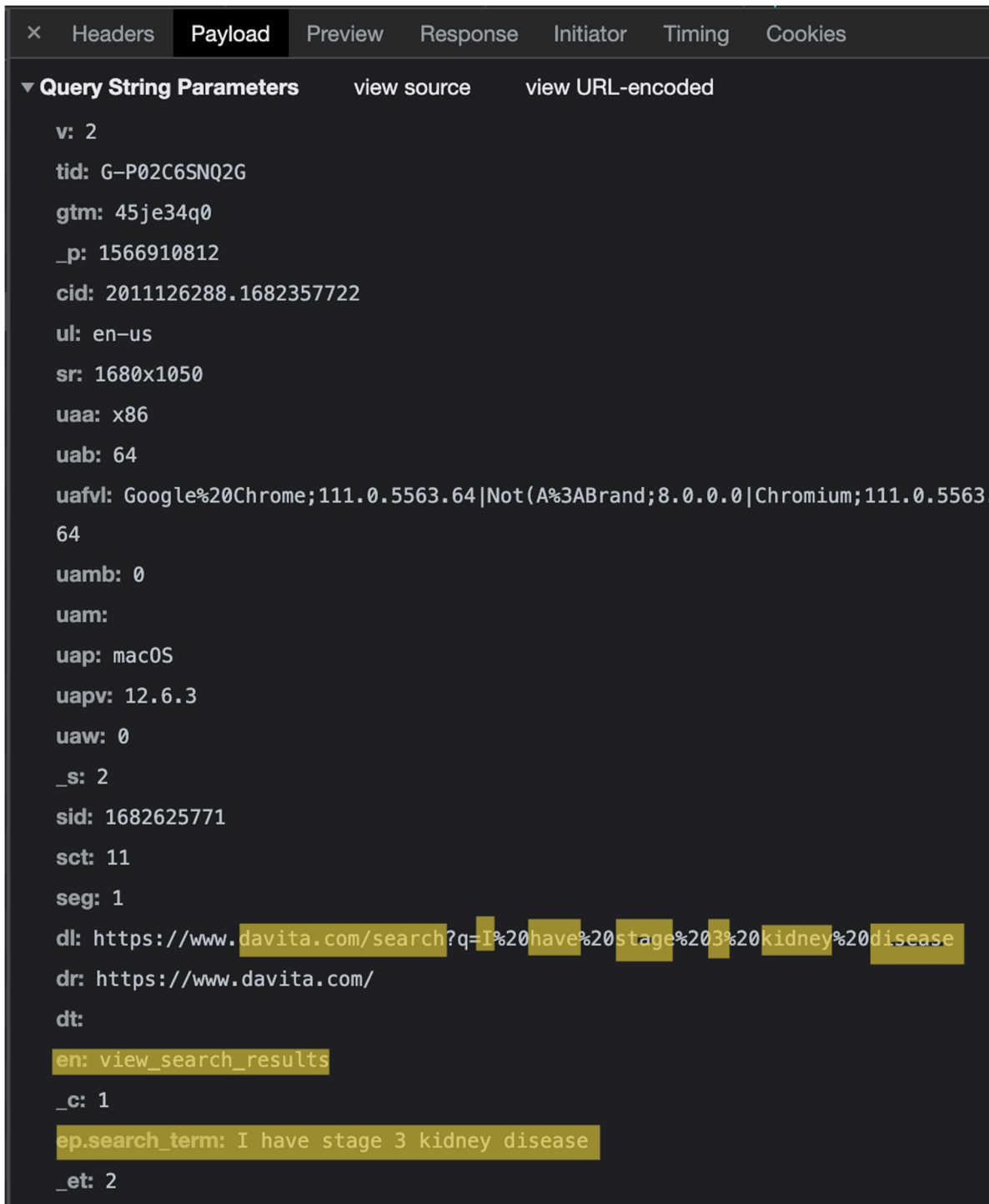
75. The image below, gathered from a users' Facebook account after using the Online Properties, plainly states "DaVita.com has shared this activity with us [74 times] using Facebook Business Tools."



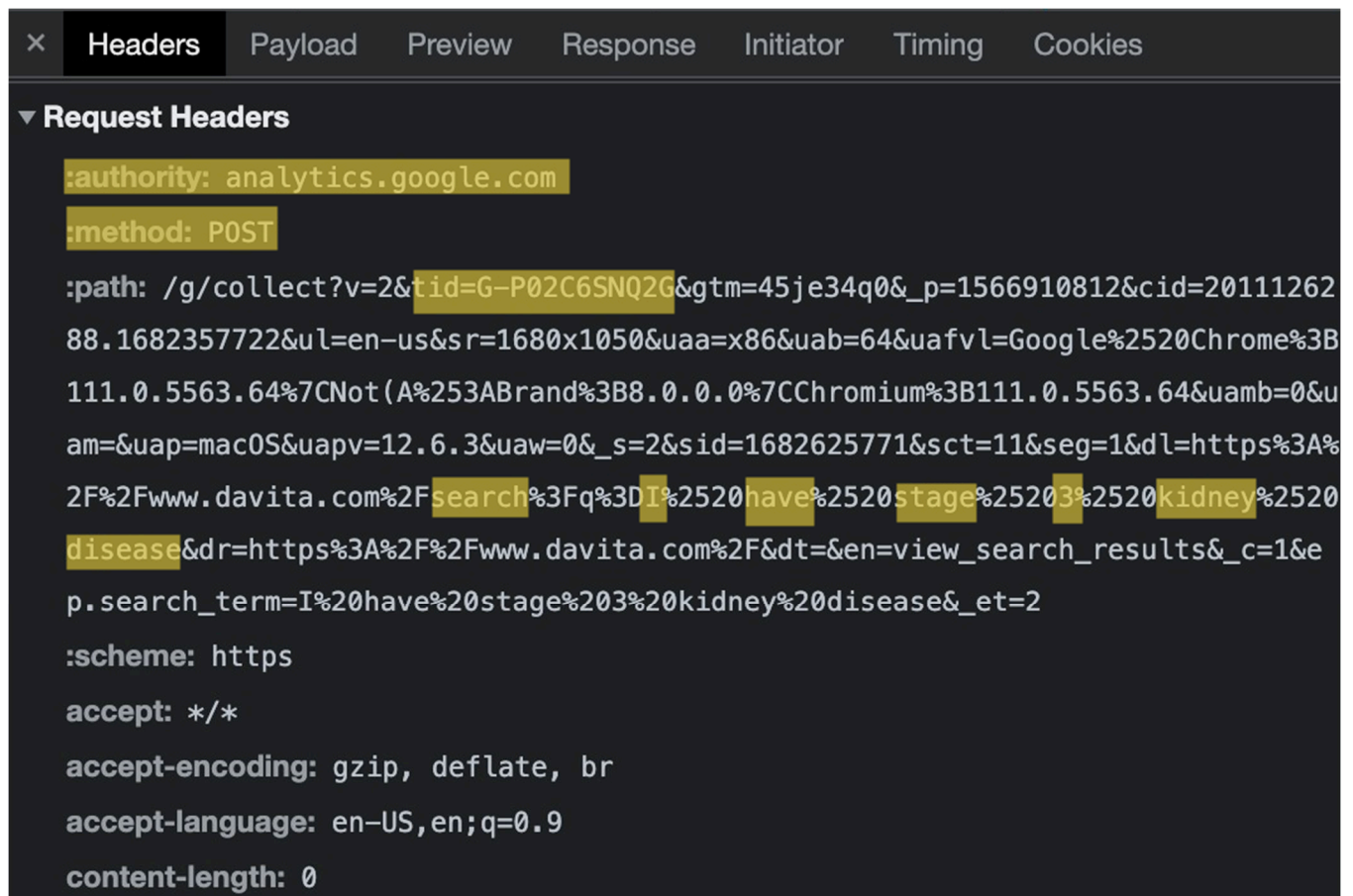
76. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but other evidence suggests it used multiple Tracking Technologies that transmitted Private Information to additional third parties.

77. The images below demonstrate that Google also received patients' Private Information via the Google Analytics tool DaVita installed and used.

78. The search phrase, “I have stage 3 kidney disease,” was received by Google alongside the user’s IP address and other persistent identifiers.



```
× Headers Payload Preview Response Initiator Timing Cookies
▼ Query String Parameters view source view URL-encoded
v: 2
tid: G-P02C6SNQ2G
gtm: 45je34q0
_p: 1566910812
cid: 2011126288.1682357722
ul: en-us
sr: 1680x1050
uaa: x86
uab: 64
uafvl: Google%20Chrome;111.0.5563.64|Not(A%3ABrand;8.0.0.0|Chromium;111.0.5563
64
uamb: 0
uam:
uap: macOS
uapv: 12.6.3
uaw: 0
_s: 2
sid: 1682625771
sct: 11
seg: 1
dl: https://www.davita.com/search?q=I%20have%20stage%203%20kidney%20disease
dr: https://www.davita.com/
dt:
en: view_search_results
_c: 1
ep.search_term: I have stage 3 kidney disease
_et: 2
```



79. This constitutes a separate and additional impermissible dissemination.

80. Like Facebook, Google views, uses, and monetizes the data it receives for marketing and links Private Information to other information in its possession.

81. In addition, upon information and belief and as described above, Defendant has also installed Conversions API on its servers to record and store its patients' Website interactions and Private Information before transmitting that information direct to Facebook via Defendant's computer server.

82. Defendant did not disclose that the Pixel, Conversions API, Google Analytics, or any other Tracking Technologies embedded in the Online Platforms' source code tracks, allows the interception of, records, and transmits Plaintiffs' and Class Members' Private Information to

Facebook and Google. Moreover, Defendant never received consent or written authorization to disclose to Facebook, Google, or other third parties the Private Information entered by Plaintiffs and Class Members via the Online Platforms.

83. Thus, without its patients' consent, Defendant effectively used its Source Code to commandeer and bug patients' computing devices, thereby re-directing their Private Information to unintended third parties (including Facebook and Google) in real time, including but not limited to, medical treatment sought, medical treatment requested at particular locations and specific dates, specific button/menu selections, content typed into free text boxes, demographic information, email addresses, phone numbers, home addresses, birth dates, insurance provider information, and emergency contact information. This Private Information relates to the past, present, or future health or health care of Plaintiffs and Class Members.

D. Plaintiffs' and Class Members' Private Information was Viewed and Used by Unauthorized Third Parties.

84. Unsurprisingly, Facebook does not offer its Pixel to companies like Defendant solely for Defendant's benefit. "Data is the new oil of the digital economy,"¹⁵ and Facebook has built its more-than \$300 billion market capitalization on mining and using that 'digital' oil. Thus, the large volumes of personal and sensitive health-related data Defendant provide to Facebook are actively viewed, examined, analyzed, curated, and used by the company. Facebook acquires the raw data to transform it into a monetizable commodity, just as an oil company acquires crude oil to transform it into gasoline. Indeed, Facebook offers the Pixel free of charge¹⁶ and the price that Defendant pay for the Pixel is the data that it allows Facebook to collect.

¹⁵ <https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/> (last visited April 25, 2023).

¹⁶ <https://seodigitalgroup.com/facebook-pixel/> (last visited April 25, 2023).

85. Facebook is a “real identity platform,”¹⁷ meaning users are allowed only one account and must share “the name they go by in everyday life.”¹⁸ To that end, when creating an account, users must provide their first and last name, date of birth, and gender.¹⁹

86. Facebook sells advertising space by emphasizing its ability to target users.²⁰ Facebook is especially effective at targeting users because it surveils user activity both on and off its own site (with the help of companies like Defendant).²¹ This allows Facebook to make inferences about users beyond what they explicitly disclose, including their “interests,” “behavior,” and “connections.”²² 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.²³

87. Advertisers can also build “Custom Audiences,”²⁴ which helps them reach “people who have already shown interest in [their] business, whether they’re loyal customers or people

¹⁷ Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

¹⁸ FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity (last visited April 5, 2023).

¹⁹ FACEBOOK, SIGN UP, <https://www.facebook.com/> (last visited April 25, 2023).

²⁰ FACEBOOK, WHY ADVERTISE ON FACEBOOK, <https://www.facebook.com/business/help/205029060038706> (last visited April 25, 2023).

²¹ FACEBOOK, ABOUT FACEBOOK PIXEL, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last visited April 25, 2023).

²² Facebook, *Ad Targeting: Help your ads find the people who will love your business*, <https://www.facebook.com/business/ads/ad-targeting> (last visited April 25, 2023).

²³ Facebook, *Easier, More Effective Ways to Reach the Right People on Facebook*, <https://www.facebook.com/business/news/Core-Audiences> (last visited April 25, 2023).

²⁴ Facebook, *About Custom Audiences*, <https://www.facebook.com/business/help/744354708981227?id=2469097953376494> (last visited April 25, 2023).

who have used [their] app or visited [their] website.”²⁵ With Custom Audiences, advertisers can target existing customers directly. 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.”²⁶ Unlike Core Audiences, Custom Audiences and Lookalike Audiences are only available if the advertiser has sent its underlying data to Facebook. This data can be supplied to Facebook by manually uploading contact information for customers or by utilizing Facebook’s “Business Tools” like the Pixel and Conversions API.²⁷

88. Facebook does not merely collect information gathered by the Pixel and store it for safekeeping on its servers without ever viewing or accessing the information. Instead, in accordance with the purpose of the Pixel to allow Facebook to create Core, Custom, and Lookalike Audiences for advertising and marketing purposes, Facebook viewed, processed, and analyzed Plaintiffs’ and Class Members’ confidential Private Information. Upon information and belief, such viewing, processing, and analyzing was performed by computers and/or algorithms programmed and designed by Facebook employees at the direction and behest of Facebook.

²⁵ Facebook, *Ad Targeting, Help your ads Find the People Who Will Love Your Business*, <https://www.facebook.com/business/ads/ad-targeting> (last visited April 25, 2023).

²⁶ Facebook, *About Lookalike Audiences*, <https://www.facebook.com/business/help/164749007013531?id=401668390442328> (last visited April 5, 2023).

²⁷ Facebook, *Create a Customer List Custom Audience*, <https://www.facebook.com/business/help/170456843145568?id=2469097953376494> (last visited April 5, 2023); Facebook, *Create a Website Custom Audience*, <https://www.facebook.com/business/help/1474662202748341?id=2469097953376494> (last visited April 5, 2023).

89. Facebook receives over 4 petabytes²⁸ of information every day and uses software that views, categorizes, and extrapolates the data to augment human effort.²⁹ This process is known as “data ingestion” and allows “businesses to manage and make sense of large amounts of data.”³⁰

90. By using data ingestion tools, Facebook can rapidly translate the information it receives from the Pixel to display relevant ads to consumers. For example, if a consumer visits a retailer’s webpage and places an item in their shopping cart without purchasing it, the next time the shopper visits Facebook, an ad for that item will appear on the shopper’s Facebook page.³¹ This evidences the fact that Facebook views and categorizes data as they are received from the Pixel.

91. Moreover, even if Facebook eventually deletes or anonymizes sensitive information that it receives, it must first view that information to identify it as containing sensitive information suitable for removal. Accordingly, there is a breach of confidentiality the instant the information is disclosed or received without authorization. As described by the HHS Bulletin:

It is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals’ authorizations requires the vendor to

²⁸ A petabyte is equal to one million gigabytes (1,000,000 GB).

²⁹ <https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4>. Facebook employees would not be able to view each piece of data individually – millions of them per second – without the aid of technology. Just as a microscope or telescope allows the user to see very small or very distant objects by zooming in, however, Facebook’s big data management software allows the company to see all this data at once by zooming out.

³⁰ <https://scaleyourapp.com/what-database-does-facebook-use-a-1000-feet-deep-dive/>. Facebook uses ODS, Scuba, and Hive to manage its massive data stores. These technologies are not traditional databases; they are specialized databases for big data designed to process data specifically for analysis—“such as [viewing] hidden patterns, correlations, market trends and customer preferences.”

³¹ *A Complete Guide to Facebook Tracking for Beginners*, OBERLO, Oct. 5, 2021, <https://www.oberlo.com/blog/facebook-pixel>.

have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.

(emphasis in original).

E. Defendant Was Enriched and Benefitted from the Use of the Tracking Technology and Private Information Had Financial Value

92. The Tracking Technologies served the sole purpose of bolstering Defendant's profits via marketing and advertising.

93. In exchange for bartering away and disclosing the Private Information of its patients, Defendant is compensated by Facebook, Google, and the like in the form of enhanced advertising services and more cost-efficient marketing on its website and Online Platforms.

94. 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.

95. By utilizing the Tracking Technologies, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

96. Defendant's disclosure of Private Information harmed Plaintiffs and the Class. Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user from mining and selling data. That figure is expected to continue to increase, and estimates for 2022 are as high as \$434 per user, constituting over \$200 billion industry wide.

97. The value of health data in particular is well-known and has been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the

extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.³²

98. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-identified patient data has become its own small economy: There’s a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers.”³³ Accordingly, patient data that can be linked to a specific individual is even more valuable.

99. Indeed, numerous marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. “No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable.”³⁴

100. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (“Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.”).

³² See <https://time.com/4588104/medical-data-industry/> (last visited April 25, 2023).

³³ See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited April 25, 2023).

³⁴ VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER <https://www.getvero.com/resources/twitter-lead-generation-cards/>. (last visited Sep. 1, 2023).

101. Several companies have products through which they pay consumers for a license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing historical information.

102. Meta also has paid users for their digital information, including browsing history. Until 2019, Meta ran a “Facebook Research” app through which it paid \$20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

103. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to \$250 per record on the black market.³⁵

F. Defendant Violated HIPAA and Industry Standards.

104. In December 2022, HHS issued a bulletin (the “HHS Bulletin”) warning regulated entities like Defendant about the risks presented by the use of Tracking Tools on their websites:

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. *For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.*³⁶

105. In other words, the HHS has expressly stated that entities who implement Tracking Tools, such as Defendant, have violated HIPAA Rules unless they have obtained a HIPAA-complaint authorization from their patients.

³⁵ Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, SecureLink (June 30, 2021), <https://www.securelink.com/blog/healthcare-data-new-prize-hackers>.

³⁶ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), available at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited October 11, 2023) (emphasis added).

106. The HHS Bulletin further warns that:

While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***³⁷

107. In addition, HHS and the FTC have recently issued a letter, once again admonishing entities like Defendant to stop using Tracking Tools:

If you are a covered entity or business associate (“regulated entities”) under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium. ***The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (e.g., tracking technology vendors) includes PHI.*** . . . Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. . . . As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app. The disclosure of such information without a consumer’s authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC’s Health Breach Notification Rule.³⁸

108. 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.³⁹

³⁷ *Id.*

³⁸ *Re: Use of Online Tracking Technologies*, U.S. Dept. of Health & Hum. Servs. and Fed. Trade. Comm’n (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

³⁹ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

109. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, “establishes national standards to protect individuals’ medical records and other individually identifiable health information (collectively defined as ‘protected health information’) and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.”⁴⁰

110. The Privacy Rule broadly defines “protected health information” (“PHI”) as individually identifiable health information (“IIHI”) that is “transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103.

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

112. Under the HIPPA de-identification rule, “health information is not individually identifiable only if”: (1) an expert “determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information” and “documents the methods

⁴⁰ HHS.gov, HIPAA For Professionals (last visited October 12, 2023), <https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html>.

and results of the analysis that justify such determination””; or (2) “the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

- (a) Names;

- (b) Medical record numbers;

- (c) Account numbers;

- (d) Device identifiers and serial numbers;
- (e) Web Universal Resource Locators (URLs);
- (f) Internet Protocol (IP) address numbers; ... and
- (g) Any other unique identifying number, characteristic, or code...; and” The covered entity must not “have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”
45 C.F.R. § 160.514.

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

114. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 (“Part C”): “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.” The statute states that a “person ... shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320d-6.

115. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

116. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall “be fined not more than \$250,000, imprisoned not more than 10 years, or both.”

117. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the HHS 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.⁴¹

118. In its guidance for Marketing, the HHS 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

⁴¹https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/De-identification/hhs_deid_guidance.pdf (last visited October 11, 2023).

marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.* (Emphasis added).⁴²

119. As alleged above, there is an HHS Bulletin that highlights the obligations of “regulated entities,” which are HIPAA-covered entities and business associates, when using tracking technologies.⁴³

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

121. Defendant's actions violated HIPAA Rules.

G. IP Addresses are Personally Identifiable Information.

122. Defendant also disclosed and otherwise assisted Facebook and Google with intercepting Plaintiffs' and Class Members' computer IP addresses.

123. An IP address is a number that identifies the address of a device connected to the Internet, and it is used to identify and route communications on the Internet.

124. Internet service providers, websites, and third-party tracking companies use individual's IP addresses to facilitate and track Internet communications.

125. Facebook tracks every IP address ever associated with a Facebook user and uses IP addresses to target individual homes and their occupants with advertising. In addition, as noted

⁴²<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/marketing.pdf> (last visited Oct. 12, 2023)

⁴³ See <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

above, Defendant use Google Analytics tools and Google Tag Manager without anonymizing users' IP addresses.

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

- 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).
- 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).

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

G. Plaintiff Victoria Witherby's Experience with Defendant's Website

128. Plaintiff Victoria Witherby is a patient that has received regular and routine medical care from Defendant on a regular basis since 2022, attends appointments each week, and she most recently scheduled and attended an appointment in or around November of 2023.

129. As a patient, and in order to obtain medical treatment from Defendant, she accessed and used its Online Platforms on her phone and desktop computer.

130. In doing so, she communicated with Defendant and its agents via Defendant's Online Platforms and reasonably expected that—as a patient seeking treatment—her communications were confidential and would not be received by Facebook, Google, and other unknown third-parties, or used for marketing purposes, without her express written consent. That was not the case.

131. Following her use of the Online Platforms, Plaintiff Witherby received targeted ads on Facebook and Instagram related to her specific medical symptoms, conditions, and treatments.

132. The timing and specificity of these and other marketing attempts is not simply a coincidence. Meta and its agents viewed and used her medical information because: (1) the targeted ads she received specifically mentioned her medical treatments she received from Defendant after using its website, scheduling medical appointments, and attending those appointments; and (2) she did not directly or purposely communicate this information to Meta or otherwise give it permission to intercept, view, or obtain her PHI from Defendant.

133. Based on the specificity of the targeted Facebook ads and emails she received at the email account associated with her Facebook, many of which referenced her exact medical symptoms and conditions, types of treatment she received from Defendant, and other details related to her past, present, and future medical history and ongoing treatment, Plaintiff Witherby believes Meta intercepted, received, learned the contents and substance of, and ultimately used her medical information.

134. Finally, Plaintiff Witherby also believes Google intercepted, received, learned the contents and substance of, and ultimately used her specific medical information because, although Defendant removed the Facebook Pixel from its Online Platforms in or around June of 2023, it has used Google Analytics in the past and also removed Google Analytics in or around June of 2023.⁴⁴ Like the Pixel, the Google Analytics tool transmits sensitive information without patients'

⁴⁴ The exact timeline for the removal of the Pixel and Google Analytics tools is presently unknown. However, DaVita made significant changes to its website in the summer of 2023 after Jane Doe filed her lawsuit, and these changes included removing or disabling Tracking Technologies and shutting down access to payment portals and portal registration.

knowledge or consent and thereby constitutes an additional impermissible disclosure of patients' medical information.

135. Notably, Plaintiff Witherby maintains and accesses her Yahoo email account ("Yahoo") on the same devices that she used to communicate with DaVita. Google acquired Yahoo, and it can identify her by name, link the information it received about her to other information in its possession (including but not limited to device identifiers), and then send her targeted advertisements. She has not, however, given Google permission to intercept, view, and otherwise receive her communications with Defendant or obtain her PHI from Defendant.

136. Plaintiff Witherby is not presently aware of the full scope of Defendant's past or continuing privacy violations, but its Online Platforms undoubtedly commandeered her web browser(s) and caused her communications to be intercepted, replicated, and obtained by Meta, Google, and other unknown third parties without her knowledge or affirmative express consent.

137. Through the process detailed in this Complaint, Defendant unlawfully assisted third parties with intercepting her communications and health information, breached confidentiality, violated her right to privacy, and unlawfully disclosed her personally identifiable information and protected health information.

138. On information and belief, Plaintiff Witherby alleges Defendant was using Tracking Technologies throughout its Online Platforms, including any password-protected patient portals and webpages, and this belief is reasonable because: (1) Defendant was in control of its Online Platforms and the source code installed, implemented, or otherwise used on its Online Platforms; (2) its use of the Pixel would have presumably been uniform across its Online Platforms, and this is supported by the fact that it was installed on sensitive appointment-booking webpages outside password-protected portions of the website or patient portals (i.e. it was being used without

regard to the sensitive nature of patients' communications); and (3) the Pixel's removal would have been uniform across its Online Platforms and would have thus been removed from password-protected webpages and portals in or around June of 2023 when Defendant received notice that its Online Platforms were impermissibly transmitting patients' and Plaintiff Witherby's protected health information to Meta via the Pixel.

139. Plaintiff Witherby has a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure and to know the precise categories of information disclosed, to whom it was disclosed, and why it was disclosed.

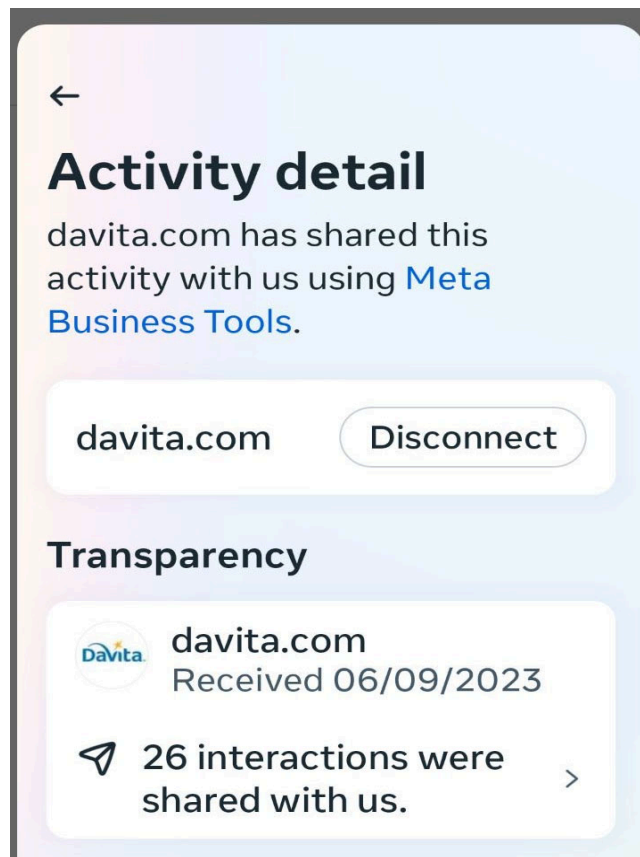
H. Plaintiff Sandra Hoover's Experience with Defendant's Online Platforms

140. Plaintiff Sandra Hoover is a patient that has received medical care from Defendant several times, on a regular basis since 2022.

141. As a patient, and in order to obtain medical treatment from Defendant, she accessed and used its Online Platforms on her phone and desktop computer to search for and identify information regarding treatment options and services provided by Defendant in relation to treating her disease, attempting to pay bills for treatments received, and information about her upcoming procedures and medical tests (including but not limited to how to prepare for those procedures and what to expect).

142. Plaintiff Hoover accessed information from Defendant and its agents via Defendant's Online Platforms and reasonably expected that—as a patient seeking treatment—her information would be confidential and would not be received by Facebook, Google, and other unknown third-parties, or used for marketing purposes, without her express written consent. That was not the case.

143. The image below is a screenshot captured by Plaintiff Hoover while accessing her personal Facebook account, specifically her “Off-Site Activity” log, which demonstrates that—at a minimum—Facebook received and viewed her communications and protected health information when she used DaVita to obtain medical care on June 9, 2023.

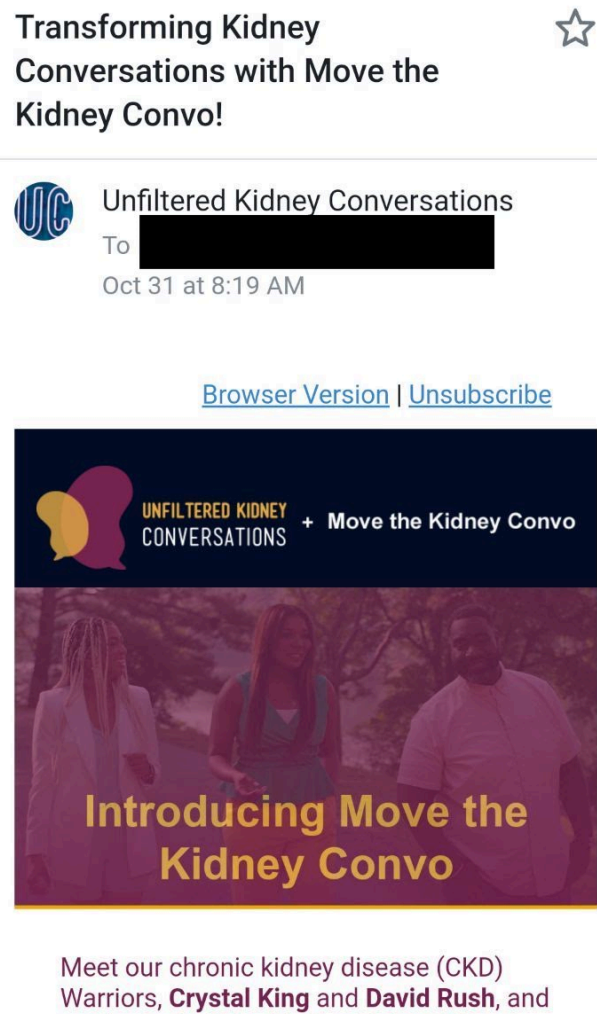


144. The image demonstrates Meta obtained and viewed her communications with Defendant (and protected health information embedded in those communications) via the Pixel, Conversions API, SDK, and related Facebook business tools—and used specific details pertaining to her health record for marketing—as a direct result of Defendant installing the Tracking Technologies and using those tools on sensitive web pages it encouraged its patients, including Plaintiff Hoover, to use in conjunction with obtaining medical care. The image also demonstrates Meta linked her Private Information to her unique Facebook account, thereby allowing Meta to

connect and associate it with other information in its possession and for retargeting and other marketing purposes.

145. Plaintiff Hoover received several targeted ads on Facebook related to her specific medical symptoms, conditions, and treatment she received from Defendant.

146. Additionally, after using the Online Platforms in conjunction with her kidney dialysis treatment, she received targeted ads and emails from a group titled “Unfiltered Kidney Conversations”:



147. Unfiltered Kidney Conversations specializes in resources for people with chronic kidney disease. However, she has never communicated directly with it or provided it with any information about her confidential medical condition.

148. Accordingly, Meta obtained, viewed, and used specific medical information concerning Plaintiff Hoover's kidney dialysis and treatment to help target her with advertisements on its platforms, and that it used the same information to deliver the specific advertisement shown above, which was received at the email address connected to her Facebook account.

149. The timing and specificity of these and other marketing attempts are not simply coincidence. Meta and its agents viewed and used her medical information, her off-site activity report specifically states that Meta will use her communications with DaVita to show her things she "might be interested in" and "relevant ads." The targeted ads she received specifically mentioned her medical symptoms, conditions, and treatments she received from Defendant after using its website, and attending appointments. She did not directly or purposely communicate this information to Meta or otherwise give it permission to intercept, view, or obtain her PHI from Defendant.

150. Based on the specificity of the targeted ads she received, many of which referenced her exact medical symptoms and conditions, types of treatment she received from Defendant, and other details related to her past, present, and future medical history and ongoing treatment, Plaintiff Hoover believes and avers Meta intercepted, received, learned the contents and substance of, and ultimately used her medical information.

151. Finally, Plaintiff Hoover also believes Google intercepted, received, learned the contents and substance of, and ultimately used her specific medical information.

152. Plaintiff Hoover is not presently aware of the full scope of Defendant's past or continuing privacy violations, but its Online Platforms undoubtedly commandeered her web browser(s) and caused her communications to be intercepted, replicated, and obtained by Meta, Google, and other unknown third parties without her knowledge or affirmative express consent.

153. Plaintiff Hoover was unaware of Defendant's use of the Pixel or any other tracking tools on its Online Platforms until approximately October of 2023.

154. Plaintiff Hoover has a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure and to know the precise categories of information disclosed, to whom it was disclosed, and why it was disclosed.

I. Plaintiff Kenneth Koskosky's Experience with Defendant's Website

155. Plaintiff Kenneth Koskosky is a patient that received regular and routine medical care in Florida from Defendant on a regular basis from 2017 through 2022, attending appointments three times a week, up until his kidney transplant in 2022.

156. As a patient, and in order to obtain medical treatment from Defendant, he accessed and used its Online Platforms on his laptop and specifically recalls reviewing information and videos related to PD dialysis treatments that DaVita encouraged him to transition to.

157. In doing so, he communicated with Defendant and its agents via Defendant's Online Platforms and reasonably expected that—as a patient seeking treatment—his communications were confidential and would not be received by Facebook, Google, and other unknown third-parties, or used for marketing purposes, without his express written consent. That was not the case.

158. In fact, following his use of the Online Platforms, he received targeted ads on Facebook and Instagram related kidney dialysis treatments he received and medical devices related to his treatment.

159. The timing and specificity of these and other marketing attempts is not simply a coincidence. Meta and its agents viewed and used his medical information because: (1) the targeted ads he received specifically mentioned his medical treatments he received from Defendant after using its website, scheduling medical appointments, and attending those appointments; and (2) he did not directly or purposely communicate this information to Meta or otherwise give it permission to intercept, view, or obtain her PHI from Defendant.

160. Finally, Plaintiff Koskosky also believes Google intercepted, received, learned the contents and substance of, and ultimately used his specific medical information because, although Defendant removed the Facebook Pixel from its Online Platforms in or around June of 2023, it has used Google Analytics in the past and also removed Google Analytics in or around June of 2023.⁴⁵ Like the Pixel, the Google Analytics tool transmits sensitive information without patients' knowledge or consent and thereby constitutes an additional impermissible disclosure of patients' medical information.

161. Notably, Plaintiff Koskosky maintains and accesses his Gmail account on the same devices that he used to communicate with DaVita. Google can identify him by name, link the information it received about him to other information in its possession (including but not limited to device identifiers), and then send him targeted advertisements. He has not, however, given

⁴⁵ The exact timeline for the removal of the Pixel and Google Analytics tools is presently unknown. However, DaVita made significant changes to its website in the summer of 2023 after Jane Doe filed her lawsuit, and these changes included removing or disabling Tracking Technologies and shutting down access to payment portals and portal registration.

Google permission to intercept, view, and otherwise receive his communications with Defendant or obtain his PHI from Defendant.

162. The risk to Plaintiffs' and other patients' privacy is ongoing in nature because the Private Information Google received can be used for years to come.

163. Plaintiff Koskosky is not presently aware of the full scope of Defendant's past or continuing privacy violations, but its Online Platforms undoubtedly commandeered his web browser(s) and caused his communications to be intercepted, replicated, and obtained by Meta, Google, and other unknown third parties without his knowledge or affirmative express consent.

164. Through the process detailed in this Complaint, Defendant unlawfully assisted third parties with intercepting his communications and health information, breached confidentiality, violated his right to privacy, and unlawfully disclosed his Private Information.

165. Plaintiff Koskosky was unaware of Defendant's use of the Pixel or any other Tracking Technologies on its Online Platforms until approximately October of 2023.

166. All three Plaintiffs suffered damages in the form of (i) invasion of privacy; (ii) diminution of value of their Private Information; (iii) statutory damages; (iv) loss of the benefit of the bargain; (v) the continued and ongoing risk to their Private Information; and (vi) the continued and ongoing risk of harassment, spam, and targeted advertisements revealing confidential information.

167. All three Plaintiffs suffer from serious chronic medical conditions that require continuous medical care. DaVita's data sharing practices, which revealed these facts, are highly offensive and simply unacceptable in civilized society. Patients are human beings with inherent rights to privacy, but they have been treated like commodities as a result of the practices described herein.

TOLLING

168. Any applicable statute of limitations has been tolled by the “delayed discovery” rule. Plaintiffs did not know (and had no way of knowing) their Private Information was intercepted and unlawfully disclosed to third parties in the manner described herein because DaVita kept this information secret, and the Tracking Tools were invisible when they used the Website.

CLASS ACTION ALLEGATIONS

169. **Class Definition:** Pursuant to Florida Rule of Civil Procedure 1.220, Plaintiffs bring this action on behalf of themselves and other similarly situated individuals (the “Class”), who, during the class period, used the Online Platforms as DaVita patients.

170. Plaintiffs reserve the right to modify the class definitions or add sub-classes as needed prior to filing a motion for class certification.

171. The “Class Period” is the period beginning on the date established by the Court’s determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgement or preliminary approval of a settlement.

172. Excluded from the Class are Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge’s staff.

173. Numerosity/Ascertainability. Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is

unknown to Plaintiffs currently. However, it is estimated that there are thousands of individuals in the Class. The identity of such membership is readily ascertainable from Defendant's records and non-party Facebook's records.

174. Typicality. Plaintiffs' claims are typical of the claims of the Class because Plaintiffs used Defendant's Online Platforms and had their personally identifiable information and protected health information disclosed to third parties such as Facebook and Google without their express written authorization or knowledge. Plaintiffs claims are based on the same legal theories as the claims of other Class Members.

175. Adequacy. Plaintiffs are fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiffs' interests are coincident with, and not antagonistic to, those of the Class Members. Plaintiffs are represented by attorneys with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically. Plaintiffs' attorneys are committed to vigorously prosecuting this action on behalf of the Class Members.

176. Common Questions of Law and Fact Predominate/Well Defined Community of Interest. Questions of law and fact common to the Class Members predominate over questions that may affect only individual Class Members because Defendant has acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. The following questions of law and fact are common to the Class:

- (a) Whether Defendant intentionally tapped the lines of internet communication between patients and their medical providers;
- (b) Whether Defendant's Online Platforms surreptitiously track personally identifiable information, protected health information, and related communications and

simultaneously discloses that information to Facebook, Google, and/or other third parties;

- (c) Whether Facebook and/or Google is a third-party eavesdropper;
- (d) Whether Defendant's disclosures of personally identifiable information, protected health information, and related communications constitute an affirmative act of communication;
- (e) Whether Defendant's conduct, which allowed third parties to view Plaintiffs' and Class Members' personally identifiable information and protected health information, resulted in a breach of confidentiality;
- (f) Whether Defendant's conduct, which allowed third parties to view Plaintiffs' and Class Members' personally identifiable information and protected health information, resulted in a breach of confidence;
- (g) Whether Defendant violated Plaintiffs' and Class Members' privacy rights by using Tracking Technologies to communicate online patients' Private Information to third parties;
- (h) Whether Plaintiffs and Class Members are entitled to damages under CIPA, the CMIA, or any other relevant statute;
- (i) Whether Defendant's actions violated the Unfair Competition Law;
- (j) Whether Defendant's actions violated Plaintiffs' and Class Members' privacy rights as provided by the California Constitution;

177. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit many similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the

unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiffs are unaware of any special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION

Common Law Invasion of Privacy – Intrusion Upon Seclusion

178. Plaintiffs repeat the allegations contained in paragraphs 1 to 177 above as if fully set forth herein and bring this count individually and on behalf of the proposed Class.

179. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Online Platforms.

180. Plaintiffs and Class Members communicated sensitive and protected medical information and individually identifiable information that they intended for only Defendant to receive and which they understood Defendant would keep private as their healthcare provider.

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

182. Plaintiffs and Class Members had a reasonable expectation that their communications, identity, health information and other data would remain confidential, and that Defendant would not install wiretaps on its Website to secretly transmit their communications to unauthorized third parties.

183. Defendant was authorized to receive Plaintiffs' and Class Members' Private Information from their respective web browsers when they used the Online Platforms, but it was not authorized to force Plaintiffs' and Class Members' web browsers to transmit information to Facebook, Google, and/or other third parties without their consent or authorization.

184. Defendant therefore obtained Plaintiffs' and Class Members' Private Information under false pretenses and/or exceeded its authority to obtain the Private Information.

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

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

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

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

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

SECOND CAUSE OF ACTION
Common Law Invasion of Privacy – Publication of Private Facts

190. Plaintiffs repeat the allegations contained in paragraphs 1 to 177 above as if fully set forth herein and bring this count individually and on behalf of the proposed Class.

191. Plaintiffs' and Class Members' Private Information, including their Internet communications and sensitive data, are private facts that Meta acquired without the knowledge or consent of Plaintiffs and Class Members.

192. Defendant gave publicity to Plaintiffs' and Class Members' Private Information and the content of their communications by sharing them with unauthorized third parties. Many of those companies have business models predicated on building massive databases of individual consumer profiles from which to sell targeted advertising and make further disseminations.

193. Plaintiffs and Class Members had no knowledge that Defendant was using software to track and disclose their Private Information because Defendant provided no information about such tracking and Plaintiffs did not otherwise consent to being tracked on third party websites.

194. Defendant's surreptitious tracking and commoditization of Plaintiffs' and Class Members' Private Information would be highly offensive to a reasonable person, particularly given that Defendant was their healthcare provider with whom they thought they were communicating confidential facts.

195. In disseminating Plaintiffs and Class Members' Private Information without their consent in the manner described above, Defendant acted with oppression, fraud, or malice.

196. Plaintiffs and Class Members have been damaged by the publication of their Private Information and are entitled to just compensation in the form of actual damages, general damages, unjust enrichment, nominal damages, and punitive damages.

THIRD CAUSE OF ACTION
Common Law– Breach of Confidence

197. Plaintiffs repeat the allegations contained in paragraphs 1 to 177 above as if fully set forth herein and bring this count individually and on behalf of the proposed Class.

CLASS ACTION COMPLAINT

198. Plaintiffs and Class Members disclosed in confidence their health and private information with Defendant through the Defendant's Website.

199. Plaintiffs and Class Members have an interest in keeping their protected private and medical information in confidence with their health services provider, the Defendant.

200. The information disclosed in confidence is protected health and private information the Defendant had knowledge was confidential due to Federal and State laws that protect such information (i.e., CIPA and HIPPA).

201. Plaintiffs and Class Members had an expectation that the confidential information disclosed to Defendant would be kept in confidence with Defendant due to their relationship with Defendant as a health services provider and Federal and State laws that protect such information (e.g., CIPA, CMIA, and HIPPA).

202. Defendant violated its duty to protect the confidentiality of Plaintiffs' and Class Members' information by using Facebook's Tracking Pixel to communicate patients' FIDs and other individually identifying information alongside their confidential medical communications with third parties, including Facebook.

203. Defendant disclosed Plaintiffs' and Class Members' confidential information for Defendant's own economic benefit in Defendant's own business and disclosing it without Plaintiffs' and Class Members' consent.

204. Defendant disclosed and disseminated Plaintiffs' and Class Members confidential communications to a broad audience including, Facebook, Google, and others.

205. At no time did Defendant offer to purchase or financially compensate Plaintiffs and Class Members for the use of their confidential information for Defendant's advertisement purposes.

206. As a result of Defendant's actions, Plaintiffs and Class Members suffered harm and injury, including but not limited to a breach of their confidence, were damaged as a direct and proximate result of Defendant's breach, and are entitled to just compensation, including monetary damages.

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

FOURTH CAUSE OF ACTION
Florida Security of Communications Act,
Florida Statutes § 934.01, et seq

208. Plaintiff Kenneth Koskosky repeats the allegations contained in paragraphs 1 to 177 above as if fully set forth herein and brings this count individually and on behalf of the proposed Class.

209. The Florida Security of Communications Act ("FSCA") is codified at Florida Statutes § 934.01, et seq. The FSCA begins with legislative findings, including:

On the basis of its own investigations and of published studies, the Legislature makes the following findings: ... (4) To safeguard the privacy of innocent persons, the interception of wire or oral communications when none of the parties to the communication has consented to the interceptions should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court.

210. Florida Statutes § 934.10 provides, in pertinent part:

Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of §§ 934.03 - 934.09 shall have a civil cause of action against any person or entity who intercepts, discloses, or uses, or procures any other person or entity to intercept, disclose, or use, such communications and shall be entitled to recover from any such person or entity which engaged in that violation such relief as may be appropriate, including: (a) [p]reliminary or equitable or declaratory relief as may be appropriate; (b) [a]ctual damages, but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher; (c) [p]unitive damages; and (d) [a] reasonable attorney's fee and other litigation costs reasonably incurred.

CLASS ACTION COMPLAINT

211. The FSCA defines “electronic communication” as “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-optical system that affects intrastate, interstate, or foreign commerce.” Fla. Stat. § 934.02(12). It further defines “intercept” as “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.” Fla. Stat. § 934.02(3).

212. At all relevant times, Defendant aided, employed, agreed with, and conspired with Facebook to intercept Plaintiffs’ and Class Members’ internet communications via the Online Platforms, including the contents thereof—i.e., the URLs visited, the medical conditions and types of treatments searched, payment of medical bills, and any other research pertaining to dialysis treatment and regime. Such information not only constitutes protected health information, it represents the substance, import, and meaning of the communications Plaintiffs and other Class members had with the DaVita website.

213. Plaintiffs and other Class members had a reasonable expectation of privacy in the electronic communications they had with the DaVita website. There was no indication given that this private medical information would be shared with others.

214. Nonetheless, these electronic communications were transmitted to and intercepted by a third party (i.e., Facebook) during the communication and without the knowledge, authorization, or consent of Plaintiffs and Class Members. That is because Defendant intentionally inserted an electronic device into its website that, without the knowledge and consent of Plaintiffs and Class members, recorded and transmitted the substance of their confidential communications with Defendant to a third party.

215. Defendant willingly facilitated Facebook's interception and collection of Plaintiffs' and Class members' private medical information by embedding the Facebook Pixel on its website.

216. Defendant used the following items as a device or apparatus to intercept wire, electronic, or oral communications made by Plaintiffs and other Class members:

- (a) The computer codes and programs Facebook used to track Plaintiffs' and Class Members' communications while they were navigating www.davita.com;
- (b) Plaintiffs' and Class Members' browsers;
- (c) Plaintiffs' and Class Members' computing and mobile devices;
- (d) Facebook's web and ad servers;
- (e) The web and ad-servers from which Facebook tracked and intercepted Plaintiffs' and Class Members' communications while they were using a web browser to access or navigate www.davita.com;
- (f) The computer codes and programs used by Facebook to effectuate its tracking and interception of Plaintiffs' and Class Members' communications while they were using a browser to visit Defendant's website; and
- (g) The plan Facebook carried out to effectuate its tracking and interception of Plaintiffs' and Class Members' communications while they were using a web browser or mobile application to visit Defendant's website.

217. Defendant fails to disclose that it is using Facebook Pixel specifically to track and automatically and simultaneously transmit communications to a third party, i.e., Facebook. Defendant is aware that these communications are confidential as privacy policy acknowledges

the confidential nature of private medical information and disclaims that it is being shared with unidentified third parties without Plaintiffs' and Class members' express authorization.

218. To avoid liability under the FSCA, a defendant must show it had the consent of all parties to a communication.

219. The patient communication information that Defendant transmits while using Facebook Pixel, such as doctor appointment booking information and names, IP addresses, and home addresses constitutes protected health information.

220. As demonstrated hereinabove, Defendant violates the FSCA by aiding and permitting third parties to receive its patients' online communications in real time through its website without their consent.

221. By disclosing Plaintiffs' and Class Members' protected health information, Defendant violated Plaintiffs' and Class members' statutorily protected privacy rights.

222. As a result of the above violations and pursuant to Florida Statutes § 934.10, Plaintiffs and Class members are entitled to actual damages or liquidated damages of \$1,000 or \$100 per day for each violation, whichever is higher.

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

224. Plaintiffs repeat the allegations contained in the foregoing paragraphs as if fully set forth therein and bring this claim individually and on behalf of the proposed Class.

FIFTH CAUSE OF ACTION
Violation Of the California Invasion of Privacy Act,
Cal. Penal Code § 630, *et seq*

225. Plaintiffs Victoria Witherby and Sandra Hoover repeat the allegations contained in paragraphs 1 to 177 above as if fully set forth herein and bring this count individually and on behalf of the proposed Class.

226. The California Invasion of Privacy Act (“CIPA”) is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose.

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

Cal. Penal Code § 630.

227. California Penal Code § 631(a) provides, in pertinent part (emphasis added):

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

228. Under CIPA, a defendant must show it had the consent of all parties to a communication.

229. At all relevant times, Defendant aided, employed, agreed with, and conspired with third parties, including Facebook and Google, to track and intercept Plaintiffs' and Class Members' internet communications while accessing Defendant's Online Platforms. These communications were transmitted to and intercepted by a third party during the communication and without the knowledge, authorization, or consent of Plaintiffs and Class Members.

230. DaVita intentionally inserted an electronic listening device onto Plaintiffs' and Class Members' web browsers that, without their knowledge and consent, tracked and transmitted the substance of their confidential communications with DaVita to Facebook, Google, and other unauthorized third parties—each of whom constitute a “person” within the meaning of the statute.

231. Defendant willingly facilitated Facebook's interception and collection of Plaintiffs' and Class Members' private medical information by embedding the Facebook Pixel on its Online Platforms. Moreover, unlike past Facebook business tools such as the Facebook Like Button and older web beacons, Defendant has full control over the Pixel, including which webpages contain the Pixel, what information is tracked and transmitted via the Pixel, and how events are categorized prior to their transmission.

232. Defendant's Tracking Technologies constitute “machine[s], instrument[s], or contrivance[s]” under the CIPA, and even if they do not, these tools fall under the broad catch-all category of “any other manner.”

233. Defendant failed to disclose its use of the Facebook Pixel, Google Analytics, or other Tracking Technologies to specifically track and automatically and simultaneously transmit Plaintiffs' and Class Members' communications with Defendant to undisclosed third parties.

234. The Tracking Technologies are designed such that they transmit a website users' actions and communications contemporaneously. As a result, the communications were intercepted in transit to the intended recipient—DaVita—before reaching DaVita's server.

235. As demonstrated hereinabove, Defendant violated CIPA by aiding and permitting third parties to intercept and receive its patients' online communications in real time as they were made via the Online Properties. Importantly, Facebook, Google, and other unauthorized third parties would not have intercepted or received the contents of these communications but for Defendant's actions and incorporations of the Analytics Code into its Online Properties.

236. By disclosing Plaintiffs' and Class Members' Private Information, Defendant violated Plaintiffs and Class Members statutorily protected right to privacy.

237. As a result of the above violations and pursuant to CIPA Section 637.2, Defendant is liable to Plaintiffs and Class Members for treble actual damages related to their loss of privacy in an amount to be determined at trial or for statutory damages in the amount of \$5,000 per violation. Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the Plaintiffs have suffered, or be threatened with, actual damages."

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

SIXTH CAUSE OF ACTION
Violation Of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56, *et seq*

239. Plaintiffs Victoria Witherby and Sandra Hoover repeat the allegations contained in paragraphs 1 to 177 above as if fully set forth herein and bring this count individually and on behalf of the proposed Class.

CLASS ACTION COMPLAINT

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

241. Defendant is a healthcare provider as defined by Cal. Civ. Code § 56.06.

242. Plaintiffs and Class Members are patients of Defendant and, as health care providers, Defendant has an ongoing obligation to comply with the CMIA’s requirements with respect to Plaintiffs’ and Class Members’ confidential medical information.

243. As set forth above, names, addresses, telephone numbers, email addresses, device identifiers, web URLs, IP addresses, and other characteristics that can uniquely identify Plaintiffs and Class Members are transmitted to Facebook and Google in combination with patient medical conditions, medical concerns, treatment(s) sought by the patients, dialysis appointments, and other patient searches and queries. This protected health information and personally identifiable information constitutes confidential information under the CMIA.

244. The Facebook ID is also an identifier that allows identification of a particular individual. Along with patients’ confidential Private Information, Defendant discloses its patients’ Facebook IDs to Facebook.

245. Pursuant to the CMIA, the information communicated to Defendant and disclosed to Facebook constitutes medical information because it is patient information derived from a health

care provider regarding patients' medical treatment and physical condition and is received by Facebook in combination with individually identifying information. Cal. Civ. Code § 56.05(i).

246. Facebook views, processes, and analyzes the confidential medical information it receives via the Facebook Tracking Pixel, Conversions API, SDKs, and other Facebook business tools. Facebook then uses the viewed confidential information to create Audiences for advertising and marketing purposes.

247. Google also views, processes, and analyzes the confidential medical information it receives via Google Analytics and then uses it for advertising and marketing purposes.

248. Defendant failed to obtain Plaintiffs' and Class Members' authorization for the disclosure of medical information.

249. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical information must: (1) be "clearly separate from any other language present on the same page and ... executed by a signature which serves no other purpose than to execute the authorization;" (2) be signed and dated by the patient or their representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date after which the authorization expires. The information set forth on Defendant's Online Platforms, including the website's Privacy Policy and Notice of Privacy Practices, does not qualify as a valid disclosure or authorization.

250. Defendant violated the CMIA by disclosing its patients' medical information to Facebook and/or Google along with the patients' individually identifying information.

251. Plaintiffs and Class Members seek nominal damages, compensatory damages, punitive damages, attorneys' fees, and costs of litigation for Defendant's violations of the CMIA.

SEVENTH CAUSE OF ACTION
Violation of the Unfair Competition Law
(Cal. Bus. & Prof. Code § 17200, *et seq.*)

252. Plaintiffs Victoria Witherby and Sandra Hoover repeat the allegations contained in paragraphs 1 to 177 above as if fully set forth herein and bring this count individually and on behalf of the proposed Class.

253. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

254. Defendant engaged in unlawful business practices in connection with its disclosure of Plaintiffs' and Class Members' Private Information to unrelated third parties, including Facebook, in violation of the UCL.

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

256. Defendant violated the "unlawful" prong of the UCL by violating, *inter alia*, Plaintiffs' and Class Members' constitutional rights to privacy, state and federal privacy statutes, and state consumer protection statutes.

257. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct, as alleged therein, offended public policy (including the federal and state privacy statutes and state consumer protection statutes, such as CIPA, CMIA, and HIPAA) and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiffs and Class Members.

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

259. Plaintiffs and Class Members suffered from a loss of the benefit of their bargain with Defendant because they overpaid for medical services that they believed included data security sufficient to maintain their Private Information as confidential.

260. As a result of Defendant's violations of the UCL, Plaintiffs and Class Members are entitled to injunctive relief. This is particularly true since the dissemination of Plaintiffs and Class Members information is ongoing.

261. As result of Defendant's violations of the UCL, Plaintiffs and Class Members have suffered injury in fact and lost money or property, including but not limited to payments to Defendant for services and/or other valuable consideration, *e.g.*, access to their private and personal data. Plaintiffs and Class Members would not have used Defendant's services, or would have paid less for them, had they known the Defendant was breaching confidentiality and disclosing their Private Information to third parties such as Facebook.

262. The unauthorized access to Plaintiffs' and Class Members' private and personal data also has diminished the value of that information.

263. In the alternative to those claims seeking remedies at law, Plaintiffs and Class Members allege that there is no plain, adequate, and complete remedy that exists at law to address Defendant's unlawful and unfair business practices. Further, no private legal remedy exists under HIPAA. Therefore, Plaintiffs and members of the proposed Class are entitled to equitable relief to restore Plaintiffs and Class Members to position they would have been in had Defendant not engaged in unfair competition, including an order enjoining Defendant's wrongful conduct,

restitution, and disgorgement of all profits paid to Defendant as a result of its unlawful and unfair practices.

RELIEF REQUESTED

Plaintiffs, on behalf of themselves and the proposed Class, respectfully requests that the Court grant the following relief:

(a) Certification of this action as a class action and appointment of Plaintiffs and Plaintiffs' counsel to represent the Class;

(b) A declaratory judgement that Defendant violated: (1) violations of Cal. Penal Code § 630, *et seq.*; (2) violations of Cal. Civ. Code § 56, *et seq.*; (3) violations of Cal. Bus. & Prof. Code § 17200, *et seq.*; (4) Violation of the Florida Security of Communications Act, Florida Statutes § 934.01, *et seq.*; (5) intrusion upon seclusion; (6) publication of private facts; and (7) breach of confidence.

(c) An order enjoining Defendant from engaging in the unlawful practices and illegal acts described therein; and

(d) An order awarding Plaintiffs and the Class: (1) actual or statutory damages; (2) punitive damages—as warranted—in an amount to be determined at trial; (3) prejudgment interest on all amounts awarded; (4) injunctive relief as the Court may deem proper; (5) reasonable attorneys' fees and expenses and costs of suit pursuant to Cal. Code of Civil Procedure § 1021.5 and/or other applicable law; (6) pre-judgment and post-judgment interest as provided by law; and (7) such other and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, demand a trial by jury for all the claims asserted in this Complaint so triable.

CLASS ACTION COMPLAINT

Date: July 2, 2024

Respectfully submitted,

/s/ Mariya Weekes

Mariya Weekes

Florida Bar No. 56299

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

201 Sevilla Avenue, 2nd Floor

Coral Gables, FL 33134

Tel: (786) 879-8200

Fax: (786) 879-7520

Email: mweekes@milberg.com

Gary M. Klinger*

gklinger@milberg.com

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN PLLC

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Tel: 866.252.0878

* *Pro Hac Vice* Forthcoming

Counsel for Plaintiffs and the Putative Class