BURSOR & FISHER, P.A.
Sarah N. Westcot (State Bar No. 264916)
701 Brickell Ave, Suite 2100
Miami, FL 33131-2800
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
E-mail: swestcot@bursor.com

Counsel for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

A.P., individually and on behalf of all others similarly situated,

Plaintiff,

v.

REAM FRANCHISE GROUP LLC, d/b/a GAMEDAY MEN'S HEALTH,

Defendant.

Case No. 3:26-cv-00433

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

A.P. ("Plaintiff") brings this action on behalf of himself, and all others similarly situated (the "Class Members"), against Defendant Ream Franchise Group LLC d/b/a Gameday Men's Health ("Defendant" or "Gameday"). Plaintiff makes the following allegations based on personal knowledge of the facts pertaining to himself, and on information and belief as to all other matters, pursuant to the investigation of his counsel.

NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of all patients who accessed and used www.gamedaymenshealth.com (the "Website") to book an appointment for men's health services.

2. Gameday is a men's health provider that is committed to redefining men's wellness by "helping men optimize their health, energy and performance."[1] Gameday has over 370 locations across the United States, including 70 locations in California.[2] Defendant also owns and operates the Website, which patients use to book appointments for various health treatments, including tri-amino acid injections, platelet-rich plasma therapy for hair loss, testosterone replacement therapy, peptides (including sermorelin, nicotinamide adenine dinucleotide, and bremelanotide), clomid, shockwave therapy, viagra, cialis, the priapus shot, vitamin injections, oral testosterone, and GLP-1 medications.

3. Confidentiality is paramount to the health industry. It is even more important when dealing with sensitive men's health issues, such as erectile dysfunction and low testosterone levels. Respecting a patient's decision to exercise their autonomy in providing personal and sensitive details about their health is vital in building trust with their clinicians.

4. "Social stigmas, the societal pressure and negative stereotypes that discourage men from seeking medical advice, significantly impact health behaviors, often deterring individuals from seeking timely medical help."[3] When booking appointments for men's health services, the

[1] *Gameday Men's Health | About*, LINKEDIN, https://www.linkedin.com/company/gameday-mens-health/about/.

[2] *Find a Clinic Near You*, GAMEDAY MEN'S HEALTH, https://gamedaymenshealth.com/location-finder.

[3] *Breaking the Silence: How Social Stigmas Impact Men's Health*, DOCGO (Jun. 28, 2024), https://docgo.com/blog/breaking-the-silence-how-social-stigmas-impact-men-s-health/; Michael

treatment is inherently personal, involving intimate details about their health struggles (e.g., erectile dysfunction and weight loss). When patients know their information is secure, they are more likely to pursue important health services.

5. As a result, patients reasonably expect sensitive and legally protected information related to their appointment will remain confidential and protected from third parties. Defendant knows that its patients expect the intimate details of their treatment to remain confidential. Such an expectation is based, in part, on legal protections afforded to such information. Being able to trust that their health information is secure is essential to upholding patient rights and the integrity of our healthcare system.

6. However, in the pursuit of profit and to the detriment of patient privacy, Defendant aids, employs, agrees, and conspires with third parties, including Google, LLC ("Google"), Zeta Global Corp. ("Zeta"), and Tiktok Ltd. ("Tiktok") (collectively, the "Third Parties"), to intercept patients' communications as they seek men's health services and book medical appointments on the Website. These tracking technologies embedded on the Website by Defendant are intentionally installed to track and disclose patient activity in real time to third parties.

7. Information related to confidential medical appointments is protected by state and federal law, including but not limited to, the California Confidentiality of Medical Information Act ("CMIA"). Healthcare providers—like Defendant—are legally required to safeguard patients' confidential and sensitive health information. These protections cover all data related to a patient's health, treatment history, and patient status. With these protections in place, patients have a reasonable expectation that protected health information ("PHI") related to their health treatment will remain confidential.

8. Despite its legal and ethical duties to maintain its patients' confidential information, Defendant instead secretly discloses Plaintiff's and Class Members' sensitive and confidential medical information with third parties. In doing so, Defendant undermines the importance of

---

Merschel, *Misguided Masculinity Keeps Many Men From Visiting The Doctor*, AMERICAN HEART ASSOCIATION (Jun. 15, 2021) https://www.heart.org/en/news/2021/06/15/misguided-masculinity-keeps-many-men-from-visiting-the-doctor.

safeguarding the identities and personal medical information of individuals seeking men's health services. Moreover, they breach the trust of patients—by violating state and federal law.

9. Unbeknownst to Plaintiff and Class Members, and contrary to Gameday Health's duties as a healthcare provider, Defendant discloses its patients' protected health information ("PHI") to third parties, including Google, Zeta, and Tiktok, for targeted advertising purposes. Due to Defendant's illegal activity, Plaintiff brings this action seeking legal and equitable remedies.

10. By failing to procure consent before enabling Third Parties to intercept these communications, Defendant violated the Electronic Communications Privacy Act ("ECPA") (18 U.S.C. §2511, et seq.), the California Invasion of Privacy Act ("CIPA") §§ 631-632, and the California Constitution.

PARTIES

Plaintiff

11. At all relevant times, Plaintiff has been a citizen of California, residing in San Francisco, California.

12. At all relevant times, Plaintiff maintained active Google and TikTok accounts. When creating his Google and TikTok accounts, Plaintiff provided Google and TikTok with his PII including his full name, date of birth, phone number, and email address. Plaintiff used the same device to access the Website that he did to access his TikTok and Google accounts. Every time Plaintiff accessed his Google and TikTok accounts, Google and TikTok collected information related to his IP address and electronic device (*e.g.*, browser, operating system, screen resolution, etc.) and stored it in a profile maintained for targeted advertising purposes. TikTok and Google also utilize other features, such as generating specific User IDs, to track its users across web browsing sessions for identification purposes, as detailed below. Google and TikTok utilize these tracking features to build robust consumer profiles they can then leverage for advertising and marketing purposes.

13. Within the last 12 months, Plaintiff navigated to Defendant's Website on multiple occasions to book medical appointments for low testosterone, including four appointments at

Defendant's Downtown San Francisco location.[4] For example, on or around February 18, 2025, Plaintiff accessed the Website to book an appointment for February 25, 2025. When booking his appointment, Plaintiff provided Defendant with his first name, last name, email address, phone number, and the reason for appointment.[5] Unbeknownst to Plaintiff, and contrary to Defendant's promise to keep patient information secure, Defendant disclosed sensitive and confidential appointment details to third parties—including Google, Zeta, and TikTok— for targeted advertising purposes. Defendant also intercepted and disclosed to Google, Zeta, and TikTok personally identifiable information ("PII") sufficient to identify Plaintiff as the precise individual booking men's health appointments.

14. After booking his appointment on the Website, Plaintiff began receiving targeted advertisements for similar products and services. However, Plaintiff was unaware, and had no way of knowing, why he was receiving such targeted advertisements. Plaintiff would not have made an appointment on the Website if he knew Defendant was sharing his PHI with unknown third parties.

Defendant

15. Defendant Ream Franchise Group LLC is a California-based limited liability company, with its principal place of business in Carlsbad, California. Defendant owns and operates the Website, which connects patients to over 400 different Gameday locations throughout the United States, including 70 locations in California.[6] Defendant chose to do so despite representing to patients that "your information is secure."

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under a law of the United States (the Electronic Communications Privacy Act, 18 U.S.C. § 2511). This Court has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367. Further, this action is a putative class action, and Plaintiff alleges that at

[4] Plaintiff used the Website to book appointments for January 16, 2025; January 28, 2025; February 25, 2025; and March 3, 2025.

[5] The specific reasons for Plaintiff's appointment have been omitted to protect his privacy.

[6] *Find a Gameday Men's Health Near You*, GAMEDAY MEN'S HEALTH, https://gamedaymenshealth.com/location-finder/.

least 100 people comprise the proposed class, that the combined claims of the proposed Class Members exceed $5,000,000 exclusive of interest and costs, and that at least one member of the proposed class is a citizen of a state different from Defendant.

17. This Court has personal jurisdiction over Defendant because Defendant purposefully directs its business activities in this District by offering its products to residents of this District and conducting a substantial amount of business in this District. Further, Plaintiff resided in this District when he accessed the Website and had the Tracking Technologies installed on his device, which Defendant knew would cause harm throughout California, including within this District.

18. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant does substantial business in this District, a substantial part of the events giving rise to the claim occurred in this District, and Plaintiff resides in this District.

FACTUAL ALLEGATIONS

A. Overview of the California Invasion of Privacy Act and the Federal Wiretap Act

19. The California Legislature enacted CIPA to protect certain privacy rights of California citizens. The California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications . . . 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.

20. The California Supreme Court has repeatedly stated the "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line *permits an outsider to tap his telephone or listen in on the call*." *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added).

21. Further, as the California Supreme Court has held in explaining the legislative purpose behind CIPA:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its *simultaneous dissemination to an unannounced*

> *second auditor, whether that auditor be a person or mechanical device.*
>
> As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas, 38 Cal. 3d at 360-61 (emphasis added; internal citations omitted); *see also Smith v. LoanMe, Inc.*, 11 Cal. 5th 183, 200 (2021) (reaffirming *Ribas*).

22. As part of CIPA, the California Legislature introduced § 631(a), which imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192 (1978). Specifically, CIPA § 631(a) prohibits any person or entity from:

> (i) "intentionally tap[ping], or mak[ing] any unauthorized connection . . . with any telegraph or telephone wire";
>
> (ii) "willfully and without the consent of all parties to the communication . . . read[ing], or attempt[ing] to read, or to learn the contents or meaning of any . . . 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 [California]"; or
>
> (iii) "us[ing], or attempt[ing] to use . . . any information so obtained."

23. CIPA § 631(a) also penalizes those who "aid[], agree[] with, employ[], or conspire[] with" or "permit[]" "any person" to conduct the aforementioned wiretapping.

24. CIPA also outlaws "us[ing] an electronic amplifying or recording device to eavesdrop upon or record [a] confidential communication." Cal. Penal Code § 632. The term "confidential communications" means "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes . . . circumstances in which the parties to the communication may reasonably expect that the communication may be overheard or recorded." Cal. Penal Code § 632(c).

25. Individuals may bring an action against a violator of CIPA §§ 631–32 for $5,000 per violation. Cal. Penal Code § 637.2.

26. In a manner similar to CIPA, the Federal Wiretap Act (i.e. the ECPA) creates "a

comprehensive scheme for the regulation of wiretapping and electronic surveillance."[7]

27. The ECPA provides "any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be punished . . . or shall be subject to suit." 18 U.S.C. § 2511 (1)(a)

28. The term "electronic communication" broadly encompasses "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 photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

29. Although the ECPA does not apply "where one part[y] to the communication has given consent[,]" the ECPA eliminates the one-party consent exception when the conduct was for the "the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."[8]

B. Defendant's Privacy Representations

30. Defendant owns and operates the Website. Unbeknownst to patients, Defendant integrates tracking codes from third parties, including Google, Zeta, and TikTok into the Website (the "Tracking Technologies").

31. When patients access the Website to book an appointment, Defendant promises its patients that "your information is secure." *See e.g.* Figure 1.

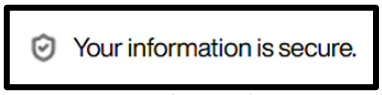

Figure 1

32. Despite this promise, Defendant intentionally intercepts and discloses patients' personally identifiable information and confidential medical information to the Third Parties.

C. Defendant Intercepted and Disclosed Sensitive, Private Information

33. Defendant intercepted information that was sensitive, confidential, and personally identifiable.

[7] *People v. Roberts*, 184 Cal. App. 4th 1149, 1167 (2010).

[8] 18 U.S.C. § 2511(d)

34. Americans have an expectation of privacy when it concerns health information. This is especially true when the disclosure of such information can reveal details of an individual's sexual and reproductive health.

35. "Testosterone is a crucial hormone that drives energy levels and motivation. . . as [you] age, however, . . . natural hormone production declines." Low testosterone can cause a variety of symptoms including loss of muscle mass, strength, and endurance; difficulty concentrate; feelings of lethargy; low libido; and erectile dysfunction.[9]

36. Not only is this confidential and sensitive, but it is also legally protected. In 2020, California passed the California Privacy Rights Act ("CPRA"), which expands the protections afforded by the California Consumer Privacy Act. This includes expanding the term "sensitive personal information" to include "[p]ersonal information collected and analyzed concerning a consumer's sex life or sexual orientation." Cal. Civ. Code § 1798.140(ae)(2)(C).

37. The California Privacy Rights Act also protects "[p]ersonal information collected and analyzed concerning a consumer's health." Cal. Civ. Code § 1798.140(ae)(2)(B).

38. The information Defendant intercepts and discloses is also protected by California's Confidentiality of Medical Information Act ("CMIA"). Cal. Civ. Code § 56.

39. Under the CMIA a "provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization,[10] except as provided in subdivision (b) or (c)." Cal. Civ. Code § 56.10(a).[11]

40. CMIA § 56.10(d) states "a provider of health care, health care service plan, contractor, or corporation and its subsidiaries and affiliates shall not intentionally share, sell, use

---

[9] *Testosterone Health: Reclaim your life with optimized testosterone*, GAMEDAY MEN'S HEALTH, https://gamedaymenshealth.com/service/testosterone-health/.

[10] The requirements for a valid authorization are set forth in Cal. Civ. Code § 56.11(b).

[11] Subdivisions (b) and (c) are not relevant to this case but permit the disclosure of medical information in situations where a government investigation or lawsuit is taking place. For example, Defendant could bypass the authorization requirement if patient medical information was requested pursuant to a lawful court order or by a party to a proceeding before a court or administrative agency pursuant to a subpoena. *See* Cal. Civ. Code §§ 56.10(b)(3) & 56.10(b)(6).

for marketing, or otherwise use medical information for a purpose not necessary to provide health care services to the patient."

41. Defendant is a provider of healthcare under the CMIA, and as a result, prohibited from disclosing medical information without a valid authorization. *See* Cal. Civ. Code § 56.06.

42. "Medical information" is defined as:

> [A]ny individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental health application information, reproductive or sexual health application information, 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, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual.

Cal. Civ. Code § 56.05(j)(1).

43. "Reproductive or sexual health application information" is defined as:

> [I]nformation about a consumer's reproductive health, menstrual cycle, fertility, pregnancy, pregnancy outcome, plans to conceive, or type of sexual activity collected by a reproductive or sexual health digital service, including, but not limited to, information from which one can infer someone's pregnancy status, menstrual cycle, fertility, hormone levels, birth control use, sexual activity, or gender identity.

Cal. Civ. Code § 56.05(q).

D. Function of Tracking Technologies

44. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each device (such as a computer, tablet, laptop, or smartphone) accesses web content through a web browser (*e.g.*, Chrome, Safari, Edge, etc.).

45. Every website is hosted by a computer server that holds the website's contents and through which the entity in charge of the website exchanges communications with the consumer's device via web browsers.

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

- HTTP Request: an electronic communication sent from a device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- Cookies: a small text file that can be used to store information on the device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.
- HTTP Response: an electronic communication that is sent as a reply to the device's web browser from the host server in response to a HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

47. A consumers' HTTP Request essentially asks the website to retrieve certain information (such as payment submissions and user selections), 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 consumer's screen as they navigate the Website).

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

49. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. The Google, Zeta, and TikTok tracking codes embedded on the Website by Defendant each constitute Source Code.

E. Google's Tracking Technologies

50. Google is one of the most valuable publicly traded companies in the world with a market capitalization of over $1 trillion dollars. Google fancies itself a "tech" company, but at its core, Google is an advertising company.

51. Google "make[s] money" from "advertising products [that] deliver relevant ads at just the right time," generating "revenues primarily by delivering both performance advertising and brand advertising."[12] In 2020, Google generated $146.9 billion in advertising revenue, which amounted to more than 80 percent of Google's total revenues for the year. Google generated an even higher percentage of its total revenues from advertising in prior years:

Table 1:

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	$257.6 billion	$209.5 billion	81.33%
2020	$182.5 billion	$146.9 billion	80.49%
2019	$161.9 billion	$134.8 billion	83.29%
2018	$136.8 billion	$116.5 billion	85.12%

52. Google offers several analytics products, including SDKs and a tracking pixel, which exist solely to help drive ad revenue. For instance, Google's SDK and pixel integrate with Google's advertising offerings, such as Google Ads, Search Ads 360, Google Cloud, and Google Ad Manager, to direct more individuals to use Google's ad network and products increasing Google's overall ad revenue. Products like Google's SDK and its tracking pixel also improve the company's advertising network and capabilities by providing more wholesome profiles and data points on individuals.

53. One of these SDKs and tracking pixels is Google Analytics. Google first launched a version of Google Analytics in 2005 as a tool for website traffic analysis. In 2007, Google launched Google Analytics Synchronous code with new tracking functionality, such as the ability to track commerce transactions. Two years later, Google launched the Google Analytics

[12] ALPHABET INC., ANNUAL REPORT (FORM 10-K) (Feb. 2, 2021), available at https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm.

Asynchronous code, which allowed webpages to load faster and improved data collection and accuracy.

54. Google continued updating its analytics platform, launching Universal Analytics in 2012. Universal Analytics offered new tracking codes and tools that provided more in-depth information about user behavior. Also, Universal Analytics enabled tracking the same user across multiple devices through its addition of the User-ID feature, which "associate[s] a persistent ID for a single user with that user's engagement data from one or more sessions initiated from one or more devices."

55. In 2020, Google launched Google Analytics 4, a platform combining Google Analytics with Firebase to analyze both app and web activity.

56. Since launching Google Analytics, Google has become one of the most popular web analytics platforms on the internet. Indeed, Google had a $62.6 billion increase in advertising revenues in 2021, compared to 2020, after launching its most recent version of Google Analytics.

57. Google touts Google Analytics as a marketing platform that offers "a complete understanding of your customers across devices and platforms."[13] It allows companies and advertisers that utilize it to "understand how your customers interact across your sites and apps, throughout their entire lifestyle," "uncover new insights and anticipate future customer actions with Google's machine learning to get more value out of your data," "take action to optimize marketing performance with integrations across Google's advertising and publisher tools," and "quickly analyze your data and collaborate with an easy-to-use interface and shareable reports."[14]

58. Google Analytics is incorporated into third-party websites and apps, including the Website, by adding a small piece of JavaScript measurement code to each page on the site. This code immediately intercepts a patient's interaction with the webpage every time the patient visits it, including what pages they visit and what they click on. The code also collects PII, such as IP addresses and device information related to the specific computing device a consumer (or patient)

[13] *Analytics*, GOOGLE, https://marketingplatform.google.com/about/analytics/ (last visited Jan. 10, 2023).

[14] *Id.*

is using to access a website. The device information intercepted by Google includes the patient's operating system, operating system version, browser, language, and screen resolution.

59. In other words, when interacting with the Website, an HTTP Request is sent to Defendant's server, and that server sends an HTTP Response including the Markup that displays the website visible to the patient and Source Code, including Google's tracking technologies.

60. Thus, Defendant is essentially handing patients a tapped device, and once the webpage is loaded onto the patient's browser, the software-based wiretap is quietly waiting for private communications on the Website to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third parties like Google.

61. Once Google's software code collects the data intercepted from the Website, it packages the information and sends it to Google Analytics for processing. Google Analytics enables the company or advertiser to customize the processing of the data, such as applying filters. Once the data is processed, it is stored on a Google Analytics database and cannot be changed.

62. After the data has been processed and stored in the database, Google uses this data to generate reports to help analyze the data from the webpages. These include reports on acquisition (e.g., information about where your traffic originates, the methods by which users arrive at your site or app, and the marketing efforts you use to drive traffic), engagement (e.g., measure user engagement by the events and conversion events that users trigger and the web pages and app screens that user visits, and demographics (e.g., classify your users by age, location, language, and gender, along with interests they express through their online browsing and purchase activities).

63. In addition to using the data collected through Google Analytics to provide marketing and analytics services, Google also uses the data collected through Google Analytics to improve its ad targeting capabilities and data points on users.

64. The Website utilizes Google's pixel and SDK. As a result, Google intercepted patients' interactions on the Website, including their PII and PHI. Google received at least "Custom Events" and URLs that disclosed the medical treatment being received by the patient.

Google also received additional PII, including the patients' IP address, device information, and User-IDs.

65. In addition to user-IDs, upon receiving information from the Website, Google also utilizes a "browser-fingerprint" to personally identify consumers. A browser-fingerprint is information collected about a computing device that is used to identify the specific device.

66. These browser-fingerprints are used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked and can provide a wide variety of data.

67. As Google explained, "[w]ith fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."[15]

68. The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it employs much more subtle techniques.[16] Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.

69. In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.[17]

70. Browser-fingerprints are personal identifiers. Tracking technologies, like the ones developed by Google and utilized on the Website, can collect browser-fingerprints from website visitors.

71. As enabled by Defendant, Google collects vast quantities of consumer data through its tracking technology.

[15] https://www.blog.google/products/chrome/building-a-more-private-web/.

[16] https://www.pixelprivacy.com/resources/browser-fingerprinting/

[17] https://ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/

72. Due to the vast network of consumer information held by Google, it is able to match the IP addresses, device information, and user-IDs it intercepts and link such information to an individual's specific identity.

73. Google then utilizes such information for its own purposes, such as targeted advertising.

74. Another tracking tool offered by Google, is the DoubleClick API.

75. The DoubleClick API "is an integrated ad technology platform that enables advertisers to more effectively create, manage and grow high-impact digital marketing campaigns."

76. DoubleClick was acquired by Google in 2008. In 2018, the DoubleClick API was integrated with the Google Analytics API into the Google Marketing Platform. The Google Marketing Platform makes use of most of DoubleClick's features, albeit under different brand names: for example, "DoubleClick Bid Manager is now Display & Video 360," "DoubleClick Search is now named Search Ads 360," and DoubleClick Campaign Manager and DoubleClick Studio are now named Campaign Manager and Studio, respectively."

77. As relevant here, however, data is still sent from the Website to Google through the DoubleClick API, and app developers like Defendant can then use the Google Marketing Platform to manage the data.

78. Once integrated into a developer's mobile application, the DoubleClick API allows an app developer to, among other features, analyze and optimize marketing campaigns and conduct targeted advertising.

79. Once Defendant intercepts the Website communications through the DoubleClick API and discloses such information to Google (in real time), Google has the capability to use such information for its own purposes. "Google uses the information shared by sites and apps to deliver [] services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalize content and ads you see on Google and on [] partners' sites and apps."

80. For example, Google utilizes the "auid" or "Advertiser User ID" cookies which identify unique users and unique interactions with a website.

81. Google also encodes the user's email address, to later match it to its own records.

82. Google's range of SaaS services is based on Google's ability to collect and analyze information about consumers' web behavior and deliver targeted advertising to select consumers based on their web habits. This involves collecting visitor information from thousands of websites and then analyzing that information to deliver targeted advertising and group web users so that they can be targeted for products and categories they are interested in.

83. Information from websites, like Defendant's Website, is central to Google's ability to successfully market their advertising capabilities to future clients.

84. In sum, Google uses website communications to: (i) improve its own products and services; (ii) develop new Google for Business and Google Analytics products and services; and (iii) analyze website visitors' communications to assist with data analytics and targeted advertising.

85. Google views and processes every piece of information collected from the DoubleClick API, including the information collected from Defendant's Website, and uses it to assist with data analytics, marketing, and targeted advertising.

86. Google partners with Defendant in its marketing efforts. Google's tracking technologies, including Google Analytics, browser fingerprinting, and Google DoubleClick are employed on the Website in the manner described throughout this Complaint.

87. Plaintiff did not authorize the interception or disclosure of his data to Google. Defendant's disclosure, and Google's interception, of Plaintiff's and prospective Class Members' PII without their consent is an invasion of privacy and violates several laws, including ECPA (18 U.S.C. § 2511, *et seq.*), CIPA § 631, CIPA § 632, and the California State Constitution.

F. Zeta's Tracking Technology

88. "The Zeta Marketing Platform unifies paid, owned, and earned media with up-to-the-minute signals, giving marketers total visibility and control to acquire, grow, and retain customers."[18]

89. Zeta markets itself to advertisers, including Defendant, as having the ability to

[18] *Zeta Marketing Platform*, ZETA, https://zetaglobal.com/platform/.

"[r]ecognize known and anonymous users across devices," "[m]ap relationships between customers and their networks to amplify impact through trusted connections," and "[a]ctivate across email, social, CTV, display, video, mobile, and in-store, and tie each touchpoint to real people and real results." [19]

90. Zeta also "combines data from anywhere in [an advertiser's] tech stack into one unified platform and extends that data with billions of signals from one of the industry's largest proprietary databases."[20]

91. Zeta's software "enables [website operators] to identify anonymous website visitors and enrich them with attributes that are unique to Zeta's 240+ million consumer profiles."[21]

92. In 2024, Zeta acquired LiveIntent,[22] wherein Zeta acquired LiveIntent's proprietary identity graph which contained more than 900 million active emails tied to over 25 billion identifiers. The graph also contains more that 100 million home IP addresses and over 400 million offline records.[23]

93. Zeta operates a number of tag domains to intercept electronic communications and personally identifiable information. Here, Defendant integrates a number of tag domains onto the Website—including but not limited to liadm.com, rlcdn.com, rezync.com, boomtrain.com; and rfihub.com into its website—to receive consumers' online activity and personally identifiable information.

94. One method of consumer data collection utilized by Defendant via the Zeta tag is its use of cookies.

95. Zeta's zync-uuid, is a universal user ID Zeta uses to for targeting and marketing to

[19] *Zeta Marketing Platform*, ZETA, https://zetaglobal.com/platform/.

[20] Melissa Tatoris, *Retail Right Now – April 2025: What's Hot, What's Changing, and What You Can't Ignore*, ZETA, https://zetaglobal.com/resource-center/retail-right-now-trends-april-2025/.

[21] *Close the Intelligence Gap and Elevate Your Marketing*, ZETA, https://zetaglobal.com/zeta-data/.

[22] *Zeta Global Completes Acquisition of LiveIntent*, ZETA, https://investors.zetaglobal.com/news/news-details/2024/Zeta-Global-Completes-Acquisition-of-LiveIntent/default.aspx.

[23] *Build your customer identity graph with LiveIntent*, LIVEINTENT: A ZETA GLOBAL COMPANY, https://www.liveintent.com/blog/build-your-customer-identity-graph-with-liveintent/

link a website user's action to Zeta's main container.[24]

96. Zeta's sd-session-id, is a user session identifier Zeta uses to for targeting and marketing to link a website user's action to Zeta's main container.[25]

97. Another cookie is the _li_ss cookie, which is a unique ID Zeta uses for re-identification[26] of consumers.[27]

98. The rud cookie is a unique ID used by Zeta for marketing and targeting; the ruds cookie is a session ID that is associated with the rud cookie.[28]

99. The eud cookie is a Partner ID cookie used by Zeta for marketing and targeting; the euds cookie is the corresponding session ID that is associated with the eud cookie.[29]

100. Defendant uses Zeta to bridge its marketing and advertising campaigns through Zeta's Customer Data Platform, including by leveraging Zeta's "single, universal persistent identifier" to link to corresponding consumer profiles, based, in part, on the aforementioned cookies.[30]

101. Zeta partners with Defendant in its marketing efforts. Zeta's tracking technologies, are employed on the Website in the manner described throughout this Complaint.

102. Plaintiff did not authorize the interception or disclosure of his data to Zeta. Defendant's disclosure, and Zeta's interception, of Plaintiff's and prospective Class Members' PII

---

[24] *Zeta Tag Domains and Cookie Classification*, ZETA, https://knowledgebase.zetaglobal.com/gswz/zeta-tags-and-cookie-domains/

[25] *Zeta Tag Domains and Cookie Classification*, ZETA, https://knowledgebase.zetaglobal.com/gswz/zeta-tags-and-cookie-domains/

[26] Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 GEO. L. TECH. REV. 202 (2017) https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017 (proliferation of publicly available information online, combined with increasingly powerful computer hardware, has made it possible to re-identify "anonymized" data).

[27] *Zeta Tag Domains and Cookie Classification*, ZETA, https://knowledgebase.zetaglobal.com/gswz/zeta-tags-and-cookie-domains/

[28] *Zeta Tag Domains and Cookie Classification*, ZETA, https://knowledgebase.zetaglobal.com/gswz/zeta-tags-and-cookie-domains/

[29] *Zeta Tag Domains and Cookie Classification*, ZETA, https://knowledgebase.zetaglobal.com/gswz/zeta-tags-and-cookie-domains/

[30] *Zeta Products and Definitions Modules*, ZETA, https://knowledgebase.zetaglobal.com/kb/zeta-product-definitions-modules.

without their consent is an invasion of privacy and violates several laws, including ECPA (18 U.S.C. §2511, *et seq.*), CIPA § 631, CIPA § 632, and the California State Constitution.

G. TikTok's Tracking Technology

103. TikTok offers an SaaS called the TikTok Pixel, which helps businesses track the performance of their ads by sending information from the business's website to TikTok, who then uses that information to optimize ad campaigns on TikTok and across the internet.[31]

104. The TikTok pixel can be "plugged in" to any website, as the pixel is a piece of code that can be added to any website to capture "events" (any activity by a user that happens on a website).

105. The TikTok Pixel is part of a package of prebuilt software tools under the "TikTok for Business" product line that allow the delivery of personalized ads. By employing TikTok to collect user information through the TikTok Pixel, websites that procure TikTok's services can use the information to deliver more effective targeted advertisements, increasing revenue for the websites.

106. In short, when users interact with a webpage with the TikTok Pixel installed, the TikTok Pixel collects the "Metadata and button clicks" (information about what the user clicked on—such as the specific URL address visited by the user— or text entered into the webpage), a timestamp for the event, and the visitor's IP address.[32] That information is sent automatically to TikTok.

107. The "TikTok for Business" business model involves entering into voluntary partnerships with various companies and surveilling communications on their partners' websites with the TikTok Pixel.

[31] "TikTok Pixel 101: What It Is & How to Use It," https://popupsmart.com/blog/tiktok-pixel (Last accessed December 27, 2023).

[32] *About TikTok Pixel*, TIKTOK BUSINESS HELP CENTER (Mar. 2025) https://ads.tiktok.com/help/article/tiktok-pixel?redirected=2).

108. Thus, through websites that employ TikTok's services, TikTok directly receives the electronic communications of website visitors entered into search bars, chat boxes, and online quizzes in real time.

109. On each page of Defendant's Website that a user visits (where the TikTok Pixel is installed), TikTok collects the URL value of the page visited, an identification code TikTok uses to track the user, and the visitor's browser type and operating system.

110. When the TikTok Pixel is used on a website, it is not like a tape recorder or a "tool" used by one party to record the other. Instead, the TikTok Pixel involves TikTok, a separate and distinct third-party entity from the parties in the conversation, using the TikTok Pixel to eavesdrop on, record, extract information from, and analyze a conversation to which it is not a party. This is so because TikTok itself is collecting the content of any conversation. That information is then analyzed by TikTok before being provided to any entity that was a party to the conversation (like Defendant).

111. Once TikTok intercepts website communications, it has the capability to use such information for its own purposes. TikTok's Commercial Terms of Service grant TikTok "a non-exclusive, royalty-free, worldwide, transferable, sublicensable license to access, use, host, cache, store, display, publish, distribute, modify and adapt [information collected from partner websites] in order to develop, research, provide, promote, and improve TikTok's products and services."[33]

112. In practice, this means the information collected is used to (i) analyze trends in consumer behavior based on data collected from websites across the internet that TikTok can then use when providing targeted advertising to other companies, (ii) create consumer profiles of specific users, allowing TikTok to sell future customers targeted advertising to consumers with specific profile characteristics, and (iii) develop new TikTok Business products and services, or improve pre-existing TikTok Business products and services.

[33] *TikTok For Business Commercial Terms Of Service*, TIKTOK FOR BUSINESS, https://ads.tiktok.com/i18n/official/policy/commercial-terms-of-service (Last updated March 2025).

113. One of TikTok's partners is Gameday. The TikTok Pixel is employed on the Website in the manner described throughout this Complaint.

114. Plaintiff did not authorize the interception or disclosure of his data to TikTok. Defendant's disclosure, and TikTok's interception, of Plaintiff's and prospective Class Members' PII without their consent is an invasion of privacy and violates several laws, including ECPA (18 U.S.C. § 2511, *et seq.*), CIPA § 631, CIPA § 632, and the California State Constitution.

H. Defendant Violates the Privacy Rights of its Patients

115. Defendant Gameday is a healthcare provider that uses the Website to connect patients to one of its nearly 400 locations across the United States.

116. As a healthcare provider, Defendant understands the information handled on its Website is protected and confidential, further indicated by its representation that patient information is secure. *Supra* Fig. 1.

117. Unfortunately, Defendant Gameday fails to comply with its legal and ethical obligations.

118. Pursuant to agreements with Google, Zeta, and TikTok, and unbeknownst to patients, Defendant intentionally and voluntarily embedded the Tracking Technologies on the Website. As illustrated within this section, Defendant unlawfully disclosed personally identifiable information and confidential medical information to Google, Zeta, and TikTok through Tracking Technologies, without patients' authorization, and contrary to its express warranty that patient information is secure.

119. The Tracking Technologies are Source Code that do just that—they surreptitiously transmit a Website User's communications and inputs to the corresponding user IDs, much like a traditional wiretap.

120. For example, when patients visit Defendant's Website via an HTTP request to Defendant's server, Defendant's server sends an HTTP response (including the Markup) that displays the webpage visible to the User, along with Source Code (including the Tracking Technologies).

121. Thus, Defendant is, in essence, handing its customers a tapped website and, once a webpage is loaded into the customer's browser, the software-based wiretaps are quietly waiting for private communications on the webpage to trigger the Tracking Technologies, which then intercept those communications—intended only for Defendant—and instantaneously disclosing those communications to Google, Zeta, and TikTok, or other third parties.

122. Third parties, including Google, Zeta, and TikTok, offer companies, including Defendant, snippets of code they can install in web browsers of users logged into their services. These code snippets uniquely identify the user and are sent with each intercepted communication to ensure the third party can identify the specific user associated with the information intercepted (in this case, confidential PII and medical information).

123. Defendant intentionally configured the Tracking Technologies installed on its Website to capture both the "characteristics" of individual's communications with its Website (their IP addresses, User-IDs, cookie identifiers, device identifiers, emails, and phone numbers) and the "content" of these communications (the buttons, links, pages, and tabs they click, and view related to reason for booking an appointment with Defendant).

124. Defendant installs these Tracking Technologies despite its understanding that its patients reasonably anticipate their identifiable information to be kept confidential and undisclosed to the Third Parties. This installation contradicts Defendant's promise to keep patient information secure.

125. Contrary to its legal and ethical duties, as soon as patients enter the Website, Defendant begins tracking and disclosing their interactions with the Website to the third parties.

126. For example, when a patient books a consultation for low testosterone, Google, through its various tracking technologies, receives the appointment location and reason, in addition to the patient's encoded email. *See* Fig. 2

//

//

//

random	1034231241
cv	11
fst	1767647450691
bg	ffffff
guid	ON
async	1
en	conversion
gtm	45be5cb0v9217444066z89226083347za20gzb9226083347zd9226083347xea
gcs	G111
gcd	13r3r3r3r5l1
dma	0
tag_exp	103116026~103200004~104527907~104528501~104684208~104684211~105391253~115583767~115938466~115938468~116184927~116184929~116251938~116251940~116682876
u_w	2560
u_h	1440
url	https%3A%2F%2Fgamedaymenshealth.com%2Fgranada-hills-ca%2Fappointment%2F
ref	https%3A%2F%2Fgamedaymenshealth.com%2Fgranada-hills-ca%2Flow-testosterone%2F
label	vexJCPHKrrIaEJvH95I_
capi	1
frm	0
tiba	Book%20Appointment%20-%20Gameday%20Men%27s%20Health%20-%20Granada%20Hills
did	dY2Q2ZW
gdid	dY2Q2ZW
edid	dY2Q2ZW
value	0
hn	www.googleadservices.com
npa	0
pscdl	noapi
auid	1400332381.1767647370
uaa	x86
uab	64
uafvl	Google%2520Chrome%3B143.0.7499.170%7CChromium%3B143.0.7499.170%7CNot%2520A(Brand%3B24.0.0.0
uamb	0
uam	
uap	Windows
uapv	19.0.0
uaw	0
ec_m	%23Email*INPUT%3Atrue%3A24%3Atrue*1
ec_sel	%23Email
ec_meta	INPUT%3Atrue%3A24%3Atrue
ec_lat	3
ec_s	1
ec_mode	a
_tu	CA
gcl_ctr	1~0
data	ads_data_redaction%3Dfalse
em	tv.1~em.XZwq3TlQcezvKEi559zeqZvo08ZXz8Rie5NCLwtirUA
fmt	3
ct_cookie_present	false
crd	CPLOsQIltN6xAgihuLECCLHBsQIlsMGxAgixw7ECCIrFsQIlwsmxAgi0xrECCPvYsQII29yxAgjZ17ECCIfbsQII08WxAgjrzLECCO3OsQII1c-xAgju0LECCJfUsQIlyduxAgjK2bECCMXcsQI
cerd	CgEA
eitems	ChElgN_tygYQq_Ss9O7yhKyTARIdAFRzg6Zt1vHx9S0_ga13ccwUTonanTJS9vdZyEc
fsk	ChElgN_tygYQpYH-_fmhwePJARIsAESDolpzTe56YF2t6YoSKh5rsA-3m2QIljf7Nb0LizhFD20Sv6vBcQiH3hwaAsbM
pscrd	IhMIq-Hk8qf1kQMVvbw6BR1-DQlYMgwIA2IICAAQABgAIAAyDAgEYgglABAAGAAgADIMCAdiCAgAEAAYACAAMgwICGIICAAQABgAIAAyDAgJYgglABAAGAAgADIMCApiCAgAEAAYACAAMgwIAmIICAAQABgAIAAyDAgLYgglABAAGAAgADIMCBViCAgAEAAYACAAMgwIH2IICAAQABgAIAAyDAgTYgglABAAGAAgADIMCBJiCAgAEAAYACAAOh5odHRwczovL2dhbWVkYXltZW5zaGVhbHRoLmNvbS9CV0NoQUlnTl90eWdZUXVkSzB2dXVabWRkY0VpMEE0YmRXSjRucTdvZmtfQ2t2UmU5NTNXTkdOM0oxTUtQYzUwVUdfT1I1ZW5Ec09tRlhsX1lWVk4zNVJRSXoMCAliCAgAEAAYACAA

Figure 2 (DoubleClick)

127. Google also receives the reason for the appointment. See, for example, Figure 3, where Google receives the service being sought by a patient (*i.e.*, testosterone health, peptide therapy, and erectile dysfunction). *See* Fig. 3.

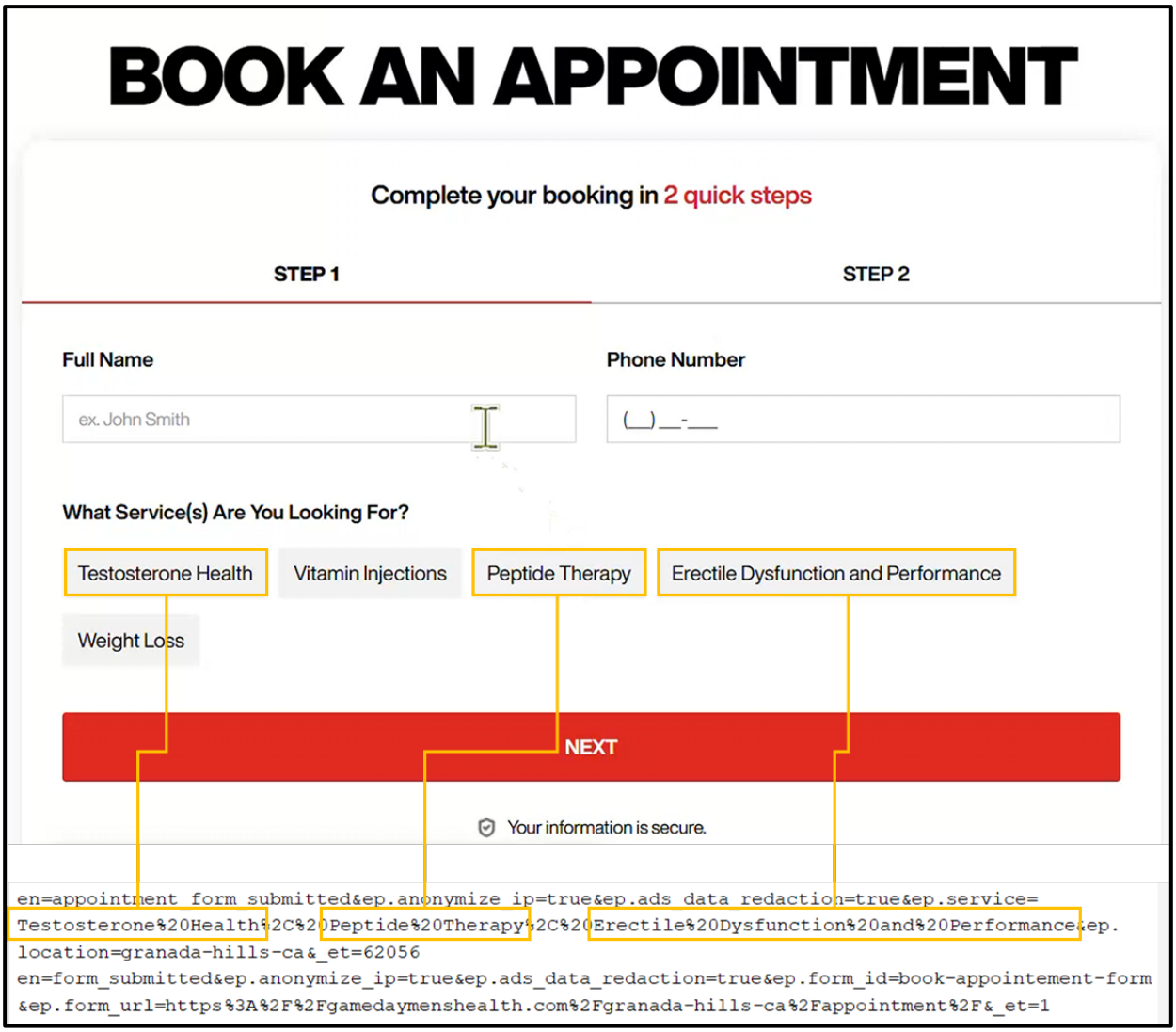

Figure 3 (Google Analytics)

//

//

//

//

//

//

128. Similarly, TikTok receives the patient's hashed phone number, hashed email, location of the appointment, and reason for booking (e.g. low testosterone). *See* Fig. 4.


```
"user": {
    "anonymous_id": "01KE7ZWFA3PNNH38JFZT7DNHMR .tt.1",
    "auto_phone_number": "b83ba9ccf537072fc493add36c6dbc76d929849417ab6c0d7cc3bec1c177030d",
    "auto_email": "5d9c2add395071ecef2848b9e7dcdea99be8d3c657cfc4627b93422f0b62ad40"
},
"pixel": {
    "code": "D3NTQIJC77U1N95E0SD0",
    "runtime": "1",
    "codes": "D3NTQIJC77U1N95E0SD0"
},
"page": {
    "url": "https://gamedaymenshealth.com/granada-hills-ca/appointment/",
    "referrer": "https://gamedaymenshealth.com/granada-hills-ca/low-testosterone/",
    "load_progress": "2"
},
"library": {
    "name": "pixel.js",
    "version": "2.2.1"
},
"session_id": "cdd37848-ea7a-11f0-ba43-020017132468::AbRy2_cNaBp2agHrF3vg",
"pageview_id": "cdd37848-ea7a-11f0-ba43-020017132468-wBHeh.4.0::f51aa9e2-ea7a-11f0-a554-08c0eb4a3a0a",
"variation_id": "traffic_1::default",
"userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36",
"index": 4,
"sessions": [{
    "csid": "1767647362374::GcNnwCl3oPyRGZDRugTl",
    "page_csid": "1767647362374::y4HpwWieQB6atWtarE0r",
    "csct": 1,
    "pixel_code": "D3NTQIJC77U1N95E0SD0"
```


Figure 4

129. Zeta, through its various endpoints, receives appointment location and reason, which it associates with various cookie values to match a website user to its own database. *See* Figs. 5–7.


```
{
    "type": "viewed",
    "site_id": "gameday-mens-health",
    "bsin":
"UzWozDaeSQPq3pOgGYDseQ76qgDhem9yvNctghIeMBhB6LkjyiZBVjuOaCpVqmWmoEqpGraOLF2s6RwOPjFsRw==",
    "userId":
"UzWozDaeSQPq3pOgGYDseQ76qgDhem9yvNctghIeMBhB6LkjyiZBVjuOaCpVqmWmoEqpGraOLF2s6RwOPjFsRw==",
    "session": "d58537fc-5a20-472c-d267-5c8ae0473a02",
    "id": null,
    "url": "https://gamedaymenshealth.com/granada-hills-ca/appointment/",
    "model": "",
    "href": "https://gamedaymenshealth.com/granada-hills-ca/appointment/",
    "properties": {
        "doc_referrer": "https://gamedaymenshealth.com/granada-hills-ca/low-testosterone/",
        "autoTrack": true,
        "track_by_url": true
    }
}
```


Figure 5 (boomtrain.com)

_li_ss	CjgKBQgKEM4cCgYI3QEQzhwKBQgMENgcCgYI9QEQzhwKBgiiARDOHAoJCP____8HENgcCgUICxDOHA
lidid	20593331-aa05-420c-b1d8-5f2169a927eb

Figure 6 (liadm.com)

Figure 7 (rezync.com)

130. At a minimum, the Zeta zync-uuid, sd-session-id, _li_ss cookie, rud cookie, ruds cookie, eud cookie, and euds cookies are enabled on the Website.

131. Defendant intercepts and discloses this information to TikTok and Google irrespective of whether a patient has an account, allowing Google and TikTok to utilize this information for their own pecuniary gain. Similarly, Defendant discloses this information to Zeta for its own targeted advertising, while permitting Zeta to use patient information for its own pecuniary gain.

132. As the owner and operator of the Website, Defendant intended for these Third Parties to receive patients' electronic communications and their personally identifiable information. And because those third parties are well-known, Defendant knew that they would use those communications for their own commercial purposes. For example, Defendant entered a contract with Zeta granting the data broker "a non-exclusive worldwide license to use the [Customer] Data for its own business and marketing purposes."[34]

133. When patients share their personal information with medical professionals, they expect this information to be kept confidential. Moreover, when consumers seek a specific treatment from medical professionals, they also expect this highly sensitive information to be kept confidential.

134. If patients knew Defendant was sharing their personal information for targeted advertising purposes, they would seek treatment with another company. Through the above-listed

[34] *Zeta Platform Agreement*, ZETA, https://zetaglobal.com/platformterms/.

third-party tracking services, which Defendant used via the software code installed, integrated, and embedded into the Website, Defendant disclosed their patients' legally protected PII and medical information.

135. Defendant engages in this deceptive conduct for its own profit at the expense of its patients' privacy. Such disclosures are an invasion of privacy, lead to harassing targeted advertising, and violating federal and state law.

I. Defendant Did Not Anonymize Patient Data By Disclosing "Hashed" Values To Third Parties

136. The Federal Trade Commission routinely evaluates privacy representations by companies. When it comes to hashing the FTC has said the following:

> Companies often claim and act as if data that lacks clearly identifying information is anonymous, but data is only anonymous when it can never be associated back to a person. If data can be used to uniquely identify or target a user, it can still cause that person harm.
>
> One way that companies obscure personal data is through "hashing." Hashing involves taking a piece of data—like an email address, a phone number, or a user ID—and using math to turn it into a number (called a hash) in a consistent way: the same input data will always create the same hash.
>
> . . .
>
> This logic is as old as it is flawed – hashes aren't "anonymous" and can still be used to identify users, and their misuse can lead to harm. Companies should not act or claim as if hashing personal information renders it anonymized. FTC staff will remain vigilant to ensure companies are following the law and take action when the privacy claims they make are deceptive.[35]

137. Thus, Defendant sent and Third Parties received Plaintiff and Class Members personally identifiable information regardless of whether it was hashed or plain text.

J. Tolling

138. Any applicable statutes of limitations have been tolled by Defendant's knowing and active concealment of its incorporation of the Tracking Technologies onto the Website.

139. The Tracking Technologies are entirely invisible to a website visitor.

[35] *No, hashing still doesn't make your data anonymous*, FEDERAL TRADE COMMISSION (Jul. 24, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous.

140. Through no fault or lack of diligence, Plaintiff and members of the putative classes were deceived and could not reasonably discover Defendant's deceptive and unlawful conduct.

141. Plaintiff and Members of the proposed class were therefore ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their part.

142. Defendant had exclusive knowledge that the Website incorporated the Tracking Technologies yet failed to disclose to its users, including Plaintiff, that by using Defendant's Website, their personally identifiable information and confidential medical information would be disclosed to third parties, including Google, Zeta, and TikTok.

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

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

145. The earliest that Plaintiff, acting with due diligence, could have reasonably discovered Defendant's conduct would have been shortly before the filing of the initial complaint in this matter.

CLASS ALLEGATIONS

146. **Class Definition:** Plaintiff brings this action individually and on behalf of various classes of persons similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

> The **Nationwide Class** that Plaintiff seeks to represent is defined as:
> All individuals residing in the United States who, during the class period, booked an appointment on the Website (the "Class" or the "Nationwide Class").
>
> The **California Subclass** that Plaintiff seeks to represent is defined as:
> All individuals residing in California who, during the class period, booked an appointment on the Website (the "California Subclass").

147. The Nationwide Class and California Subclass are referred to collectively as the

"Classes."

148. Subject to additional information obtained through further investigation and discovery, the above-described Classes may be modified or narrowed as appropriate, including through the use of subclasses.

149. The "Class Period" is the time 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 judgment.

150. Excluded from the proposed Classes 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.

151. **Numerosity:** Members of the Classes are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiff at this time. However, it is estimated that there are at least thousands of individuals in the Classes. The identity of such membership is readily ascertainable from Defendant's and Third Parties' records.

152. **Typicality:** The claims of the named Plaintiff are typical of the claims of the Classes because the Plaintiff, like all other Class Members, used the Website to schedule a medical appointment and had his personally identifiable information and protected medical information disclosed to the Third Parties without his express written authorization or knowledge. Plaintiff's claims are based on the same legal theories as the claims of other Class Members.

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

154. **Commonality:** Questions of law and fact common to the members of the Classes predominate over questions that may affect only individual members of the Classes because Defendant has acted on grounds generally applicable to the Classes. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Classes include::

a. Whether Defendant intentionally tapped the lines of internet communication between patients and their healthcare provider;

b. Whether the Website surreptitiously recorded personally identifiable information, protected medical information, and related communications and subsequently, or simultaneously, disclosed that information to Third Parties, including Google, Zeta, and TikTok;

c. Whether Google is a third-party eavesdropper;

d. Whether Zeta is a third-party eavesdropper;

e. Whether TikTok is a third-party eavesdropper;

f. Whether Defendant's disclosures of personally identifiable information, protected medical information, and related communications constituted an affirmative act of communication;

g. Whether Defendant's conduct, which allowed Google, Zeta, and TikTok—unauthorized parties—to view Plaintiff's and Class Members' personally identifiable information and protected medical information, resulted in a breach of confidentiality;

h. Whether Defendant violated Plaintiff's and Class Members' privacy rights by using the Tracking Technologies to record and communicate patients' confidential medical communications;

i. Whether Plaintiff and Class Members are entitled to damages under the ECPA, CIPA, or any other relevant statute;

j. Whether Defendant's actions violated Plaintiff's and Class Members' privacy rights as provided by the California Constitution; and

k. Whether Plaintiff and members of the proposed Classes are entitled to damages, reasonable attorneys' fees, pre-judgment interest and costs of this suit.

155. **Superiority:** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of the Classes. Each individual Class Member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues. Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby making it appropriate for this Court to grant final injunctive relief and declaratory relief with respect to the Classes as a whole. Finally, Plaintiff knows of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

COUNT I
Violation Of The Electronic Communication Privacy Act,
18 U.S.C. § 2511, *et seq.*
(On Behalf of the Nationwide Class)

156. Plaintiff incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

157. Plaintiff brings this claim on behalf of himself and members of the Nationwide Class.

158. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

159. The ECPA protects both the sending and the receipt of communications.

160. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

161. The transmission of Plaintiff's sensitive and personal information to Defendant's website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

162. The transmission of PII between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

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

164. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

165. The ECPA defines "electronic, mechanical, or other device," as "any device . . . which can be used to intercept a[n] . . . electronic communication[.]" 18 U.S.C. § 2510(5).

166. The following instruments constitute "devices" within the meaning of the ECPA:

a. The computer codes and programs Defendant and Google used to track Plaintiff's and Class Members' communications while they were navigating the Website;

b. The computer codes and programs Defendant and Zeta used to track Plaintiff's and Class Members' communications while they were navigating the Website;

c. The computer codes and programs Defendant and TikTok used to track Plaintiff's and Class Members' communications while they were navigating the Website;

d. Plaintiff's and Class Members' browsers;

e. Plaintiff's and Class Members' mobile devices;

f. Defendant's and Google's web and ad servers;

g. Defendant's and Zeta's web and ad servers;

h. Defendant's and TikTok's web and ad servers;

i. The plan that Defendant and Google carried out to effectuate the tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to navigate the Website;

j. The plan that Defendant and Zeta carried out to effectuate the tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to navigate the Website;

k. The plan that Defendant and TikTok carried out to effectuate the tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to navigate the Website.

167. Plaintiff's and Class Members' interactions with Defendant's website are electronic communications under the ECPA.

168. By utilizing and embedding the tracking technologies provided by the Third Parties on the Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class Members in violation of 18 U.S.C. § 2511(1)(a).

169. Specifically, Defendant intercepted—in real time—Plaintiff's and Class Members' electronic communications via the tracking technologies provided by the Third Parties on its Website, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' PII and sensitive and personal health information to the Third Parties.

170. The Defendant intercepted communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class Members regarding their PII, including their identities and information related to their purchase on the Website. This confidential information is then monetized for targeted advertising purposes, among other things.

171. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class

Members' electronic communications to the Third Parties through the Tracking Technologies, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

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

173. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, invasion of privacy.

174. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

175. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may award statutory damages to Plaintiff and Class Members; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future; reasonable attorney's fees; and other litigation costs reasonably earned.

COUNT II
Violation Of The California Invasion Of Privacy Act, Cal. Penal Code § 631
(On Behalf of the California Subclass)

176. Plaintiff incorporates by reference the preceding paragraphs as if fully set forth herein.

177. Plaintiff brings this claim against Defendant individually and on behalf of the California Subclass.

178. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§

630–638. CIPA begins with its statement of purpose—namely, that the purpose of CIPA is to "protect the right of privacy of the people of [California]" from the threat posed by "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications . . . ." Cal. Penal Code § 630.

179. A person violates California Penal Code § 631(a), if:

> By means of any machine, instrument, or contrivance, or in any other manner, [s/he] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable or instrument of any internal telephonic communication system, or [s/he] 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 [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained . . . .

Cal. Penal Code § 631(a).

180. Further, a person violates § 631(a) if s/he "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" in the preceding paragraph. *Id.*

181. To avoid liability under § 631(a), a defendant must show it had the consent of <u>all</u> parties to a communication.

182. At all relevant times, Defendant aided, agreed with, and conspired with to track and intercept Plaintiff's and Class Members' internet communications while accessing the Website. These communications were intercepted without the authorization and consent of Plaintiff and Class Members

183. Defendant, when aiding and assisting the Third Parties' wiretapping and eavesdropping, intended to help the Third Parties learn some meaning of the content in the URLs and the content the visitor requested.

184. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the Tracking Technologies fall under the broad catch-all

category of "any other manner":

a. The computer codes and programs Google, Zeta, and TikTok used to track Plaintiff and Class Members' communications while they were navigating the Website;

b. Plaintiff's and Class Members' browsers;

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

d. Google's web and ad servers;

e. Zeta's web and ad servers;

f. TikTok's web and ad servers;

g. The web and ad-servers from which Google, Zeta, and TikTok tracked and intercepted Plaintiff's and Class Members' communications while they were using a web browser to access or navigate the Website;

h. The computer codes and programs used by Google, Zeta, and TikTok to effectuate their tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit the Website; and

i. The plan Defendant and Google carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to visit the Website;

j. The plan Defendant and Zeta carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to visit the Website.

k. The plan Defendant and TikTok carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to visit the Website.

185. The information that Defendant transmitted using Tracking Technologies constituted sensitive and confidential personally identifiable information.

186. As demonstrated hereinabove, Defendant violated CIPA by aiding and permitting the Third Parties to receive its patients' sensitive and confidential online communications through

the Website without their consent.

187. As a result of the above violations, Defendant is liable to Plaintiff and other Class Members in the amount of, the greater of, $5,000 per violation or three times the amount of actual damages. Additionally, Cal. Penal Code § 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered or be threatened with, actual damages." Under the statute, Defendant is also liable for reasonable attorney's fees, and other 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 Defendant in the future.

COUNT III
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 632
(On Behalf of the California Subclass)

188. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

189. Plaintiff brings this claim against Defendant individually and on behalf of the California Subclass.

190. Cal. Penal Code § 632 prohibits "intentionally and without the consent of all parties to a confidential communication," the "use[] [of] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication.

191. Section 632 defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto[.]"

192. The data collected on Defendant's Website constitutes "confidential communications," as that term is used in Section 632, because Class Members had an objectively reasonable expectation of private with respect to their personally identifiable information.

193. Plaintiff and Class Members expected their communications to Defendant to be confined to Defendant in part, because of Defendant's consistent representations that these communications would remain confidential. Plaintiff and Class Members did not expect third

parties—such as Google, Zeta, and TikTok—to secretly eavesdrop upon or record this information and their communications.

194. The Tracking Technologies from Google, Zeta, and TikTok, are electronic amplifying or recording devices for purposes of § 632.

195. By contemporaneously intercepting and recording Plaintiff's and Class Members' confidential communications to Defendant through this technology, third parties, including Google, Zeta, and TikTok eavesdropped and/or recorded confidential communications through an electronic amplifying or recording device in violation of § 632 of CIPA.

196. At no time did Plaintiff or Class Members consent to Defendant's, Google's, Zeta's, or TikTok's conduct, nor could they reasonably expect that their communications to Defendant would be overheard or recorded by Google, Zeta, and TikTok.

197. Google, Zeta, and TikTok utilized Plaintiff's and Class Members' personally identifiable information for their own purposes, including advertising and analytics.

198. Defendant is liable for aiding and abetting violations of Section 632 by Google, Zeta, and TikTok.

199. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Members of the California Subclass have been injured by the violations of Cal. Penal Code § 632, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT IV
Invasion of Privacy Under California's Constitution
(On Behalf of the California Subclass)

200. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

201. Plaintiff brings this claim against Defendant individually and on behalf of the California Subclass.

202. Plaintiff and Class Members have an interest in: (1) precluding the dissemination of their sensitive, confidential online communications; and (2) making personal decisions and/or conducting personal activities without observation, intrusion, or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

203. At all relevant times, by using the Tracking Technologies to record and communicate their sensitive and confidential online communications, Defendant intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

204. Plaintiff and Class Members had a reasonable expectation that their sensitive and confidential online communications, identities, health information, and other data would remain confidential and that Defendant would not install wiretaps on the Website .

205. Plaintiff and Class Members did not authorize Defendant to record and transmit Plaintiff's and Class Members' sensitive confidential online communications.

206. The invasion of privacy was serious in nature, scope, and impact because it related to their sensitive and private online communications. Moreover, it constituted an egregious breach of societal norms underlying the privacy right because Defendant promised to keep Plaintiff and Members of the California Subclass's communications confidential.

207. Accordingly, Plaintiff and members of the California Subclass seek all relief available for invasion of privacy claims under California's Constitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order certifying the putative Nationwide Class and California Subclass defined above, naming Plaintiff as the representative of the putative Classes, and naming Plaintiff's attorneys as Class Counsel to represent the putative Class and Subclass Members;

(b) For an order declaring that the Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiff and the putative Classes on all counts asserted herein;

(d) For statutory damages in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For injunctive relief as pleaded or as the Court may deem proper; and

(g) For an order awarding Plaintiff and the putative Classes their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff hereby demands a trial by jury for any and all issues in this action so triable of right.

Dated: January 15, 2026

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Sarah N. Westcot*
Sarah N. Westcot

Sarah N. Westcot (State Bar No. 264916)
701 Brickell Ave, Suite 2100
Miami, FL 33131-2800
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
E-mail: swestcot@bursor.com

Counsel for Plaintiff

ClassAction.org
