Filing # 253264249 E-Filed 07/24/2026 07:41:10 PM

IN THE CIRCUIT COURT OF THE 17TH JUDICIAL CIRCUIT IN AND FOR BROWARD COUNTY, FLORIDA

JUSTIN BREWER, ARIEL BROOKS ALEX SISTI, and MARC WEINBERGER, individually, and on behalf of all others similarly situated,

Plaintiffs,

v.

CVS PHARMACY, INC., CRITEO CORP. and MEDALLIA, INC.,

Defendants.

CASE NO. CACE-26-008094

CLASS REPRESENTATION

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Justin Brewer, Ariel Brooks, Alex Sisti, and Marc Weinberger (collectively, "Plaintiffs") file this Amended Class Action Complaint on behalf of themselves and all others similarly situated against CVS Pharmacy, Inc. ("CVS") and Criteo Corp. ("Criteo") (collectively, "Defendants"). Plaintiffs make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to the allegations specifically pertaining to themselves, which are based on personal knowledge.

NATURE OF THE ACTION

1. CVS, which has over 36 million customers, maintains an online pharmacy, retail store for over-the-counter medical products, vaccination center, and health clinic, all through its website, www.cvs.com ("Website"), and its CVS Pharmacy mobile application, which is offered on both iOS and Android devices (the "App").[1]

[1] The Application shall refer to both the iOS and Android versions, unless otherwise specified.

2. CVS encourages Website and Application users, including Plaintiffs and Class Members, to use the Website and Application to search for and purchase over-the-counter medications and healthcare products, schedule vaccine administrations, manage prescriptions, schedule in-person and virtual doctor appointments via the MinuteClinic Services, and take other actions related to their personal healthcare. While doing this, Website and Application users, including Plaintiffs and Class Members, conveyed private information, including medical information, to CVS.

3. CVS' Pharmacy and Consumer Wellness segment, as of December 31, 2024, filled 1.7 billion prescriptions and dispensed approximately 27% of total retail pharmacy prescriptions in the United States.

4. Plaintiffs and all other Class Members are users who communicated with CVS through the Website and/or App. They shared information, including their Protected Health Information ("PHI") and Personally Identifiable Information ("PII") (together, "Private Information"), with the reasonable belief that CVS would take appropriate steps to maintain the privacy of these communications.

5. Instead, CVS did the opposite, aiding, employing, agreeing, and conspiring with Adobe, Inc. ("Adobe"), Criteo, Medallia, Quantum Metric, Inc. ("QM") (collectively, "Third-Party Trackers") and others to intercept, eavesdrop, and/or record sensitive and confidential personal and medical communications of Website users via third-party code embedded on the Website.

6. Criteo is a digital advertising company that focuses on serving personalized advertisements. In 2024, Criteo and Criteo S.A. reported approximately $1.9 billion in revenue. Criteo describes itself as partnering with some of the largest and most sophisticated consumer

brands, retailers, commerce companies and media owners in the world "to capture user activity on their websites and mobile applications […], which we define as digital properties, and leverage that data to deliver superior ad performance to help marketers, brands and agencies reach their campaign objectives from top to bottom of the marketing funnel."

7. Medallia is a multi-faceted digital advertising and data analysis company that focuses on collecting, compiling, and processing its clients' customer and employee data. Medallia describes its digital solutions as permitting customers to "identify who is visiting your digital property and what they want while powering individualized next/best actions across your organization For example, it touts that its Total Experience Profile can "bring together data from every experience to create a complete timeline of every interaction a customer has with your company—whether online, by phone, via chat, or in person," empowering companies to "provide personalized service, orchestrate better omni-channel programs, and create more relevant campaigns powered by experience-based segmentation."

8. Through the third-party code it implemented on the Website and App, CVS has, unbeknownst to Plaintiffs and without their consent, enabled the Third-Party Trackers' interception, eavesdropping, and/or recording of information about Plaintiffs' and Class Members' medical conditions, immunizations and vaccines, prescriptions, and other Private Information, including their activity searching for and purchasing sensitive healthcare products.

9. Accordingly, Plaintiffs bring this action on behalf of themselves and a Class of all persons who used the CVS Website and/or Application and had their electronic communications were intercepted or recorded by the Third-Party Trackers, as enabled by CVS.

THE PARTIES

10. Plaintiff Marc Weinberger is an adult citizen of the state of Florida and resides in

Boca Raton, Florida.

11. On multiple occasions within the past year, Plaintiff Weinberger visited CVS' Website and, through his interactions with the Website, provided his Private Information to CVS, including searching for and viewing sensitive health-related products on the Website.

12. Specifically, Plaintiff Weinberger used the Website for things like researching over-the-counter medical products relating to a medical condition affecting Plaintiff. Plaintiff searched for these over-the-counter products on the Website and viewed the corresponding product pages after performing his searches for these medications. Plaintiff Weinberger also purchased health products after viewing them on the Website.

13. Plaintiff Ariel Brooks is an adult citizen of the state of California and resides in Oakland, California.

14. In or around October 2024, prior to the filing of this lawsuit, Plaintiff Brooks used the Application to browse over-the-counter medications, and refill her prescription medications.

15. Plaintiff Brooks has been accessing her account on the Application since at least February 2024. During the October visit, Defendants enabled QM to intercept Plaintiff Brooks' electronic communications with CVS in real-time, including but not limited to, her first and last name, email address, physical address, medications, and products that she viewed. Plaintiff Brooks was unaware at the time that her electronic communications, including the information described above, were being intercepted in real-time and disclosed to QM, nor did Plaintiff Brooks consent to the same.

16. Plaintiff Brooks was not aware of the tracking technology operating on the Application and did not consent to CVS' disclosure of her Private Information as described above.

17. Plaintiff Brooks reasonably expected her communications with CVS via the

Application to be confidential, and that such communications would not be transmitted to or intercepted by QM, or other third parties in a personally identifiable manner without disclosure to her and her corresponding express consent.

18. By failing to receive the requisite consent, CVS breached its duty of confidentiality and aided the Third-Party Trackers in unlawfully intercepting Plaintiff's Private Information. Such acts are egregious violations of Plaintiff's right to and reasonable expectation of privacy.

19. Plaintiff Justin Brewer is an adult citizen of the state of California and resides in San Jacinto, California.

20. On multiple occasions within 2025, Plaintiff visited CVS' Website and, through his interactions with the Website, provided his Private Information to CVS, including searching for and viewing sensitive health-related products on the Website.

21. Specifically, Plaintiff Brewer used the Website for things like researching over-the-counter medical products relating to a serious medical condition affecting Plaintiff and relating to private sexual health products. Plaintiff searched for these over-the-counter products on the Website and viewed the corresponding product pages after performing his searches for these medications. Plaintiff Brewer also purchased sexual health products after viewing them on the Website.

22. As a result of Defendants' conduct, Plaintiff Brewer received targeted advertisements as he browsed online webpages, both on the Website and on other websites, relating to his private activity on the Website. Specifically, after searching on the Website for products related to his medical condition, Plaintiff saw advertisements for medications relating to that medical condition and related symptoms. He also saw advertisements for similar sexual health products as those he purchased on the Website.

23. Whenever Plaintiff Brewer has used the Website, he has used it as a "guest." Mr. Brewer has not created an account on the Website.

24. Plaintiff Brewer was not aware of the tracking technology operating on the Website and did not consent to CVS' disclosure of his Private Information as described above.

25. Plaintiff Brewer reasonably expected his communications with CVS via the Website to be confidential, and that such communications would not be transmitted to or intercepted by Adobe, Criteo, Medallia, or other third parties in a personally identifiable manner without disclosure to him and his corresponding express consent.

26. Plaintiff Alex Sisti is an adult citizen of the state of Maryland and resides in Laurel, Maryland. On multiple occasions in 2025, prior to the filing of this lawsuit, Plaintiff Sisti used the Application to fill his prescription medications.

27. Defendants enabled QM to intercept Plaintiff Sisti's electronic communications with CVS in real-time, including but not limited to, his first and last name, email address, physical address, medications, and products that he viewed. Plaintiff Sisti was unaware at the time that his electronic communications, including the information described above, were being intercepted in real-time and disclosed to QM, nor did Plaintiff Sisti consent to the same.

28. Plaintiff Sisti was not aware of the tracking technology operating on the Application and did not consent to CVS' disclosure of his Private Information as described above.

29. Plaintiff Sisti reasonably expected his communications with CVS via the Application to be confidential, and that such communications would not be transmitted to or intercepted by QM, or other third parties in a personally identifiable manner without disclosure to him and his corresponding express consent.

30. Defendant CVS Pharmacy, Inc. is a Delaware corporation with its principal

executive offices located at One CVS Drive, Woonsocket, Rhode Island.

31. Defendant Criteo Corp. is a Delaware corporation with its principal executive offices and principal place of business located in New York, New York.

JURISDICTION AND VENUE

32. The Court has subject-matter jurisdiction pursuant to Florida Rule of Civil Procedure 1.220 and Fla. Stat. § 26.012(2). The matter in controversy exceeds the sum or value of $30,000.00, exclusive of interest, costs, and attorneys' fees. It is estimated that the members of the proposed class number in the millions.

33. This case is appropriately complex as to be subject to the jurisdiction of the Complex Business Division pursuant to Administrative Order 2017-35-CIV (6)(c), as it is a class action complaint, the amount in controversy exceeds $150,000.00, exclusive of interest, costs, and attorneys' fees, and involves the sale of services by a business entity.

34. The Court has jurisdiction over Defendant because Defendant conducts substantial business within Florida, such that Defendant has significant, continuous, and pervasive contacts with the state of Florida.

35. Venue is proper in this Court because numerous class members reside in this County and the facts giving rise to this action occurred in this County.

STATEMENT OF FACTS

A. OVERVIEW OF QM'S SERVICES

36. QM provides a software-as-a-service platform of the same name to customers across the country, including CVS.

37. QM's service includes many features such as data analytics, AI analysis, and session replay. Each of these features is employed by CVS on the Application and is discussed in

turn.

1. Session Replay

38. Most relevant to this action is QM's "Session Replay" function. As QM describes Session Replay on its website:

> Session replay is the reproduction of a user's interactions on web or native mobile applications. Session replay captures things like mouse movements, clicks, typing, scrolling, swiping, tapping, etc. Session replay isn't a recording of a user's session. It's a reproduction of the individual experience based on the changing state of their browser or application, with all of the underlying contextual user data.[2]

39. QM's patented "capture method" "provides the ability to capture any native application screen or view and translate those components into familiar DOM counterparts to render them in our replay engine."[3]

40. In more technical terms, a crucial component of every website is the Document Object Model ("DOM"), which "is the data representation of the objects that comprise the structure and content of a document on the web."[4] In other words, the DOM is part of the foundation of any given website or application.

41. When a user interacts with an application—such as by clicking on particular item of interest or entering text into a search bar—the DOM is altered. Session replay services like QM's "log[] every change made to the DOM, such as users entering or retrieving information, as an event. [They] then string[] these events together into a representation of each user's individual session."[5]

---

[2] https://www.quantummetric.com/platform/session-replay/.
[3] https://www.quantummetric.com/platform/mobile-app-analytics.
[4] https://developer.mozilla.org/en-US/docs/Web/API/Document_Object_Model/Introduction.
[5] https://www.datadoghq.com/knowledge-center/session-replay/.

42. After capturing the event data (*e.g.*, items clicked or text entered), session replay services like QM's compile this information into a "video recording" of the user's visit to the website. As a result, companies can "can pause, rewind, and fast-forward the session (just like a YouTube video) to watch how a user interacts with a website or mobile app."[6]

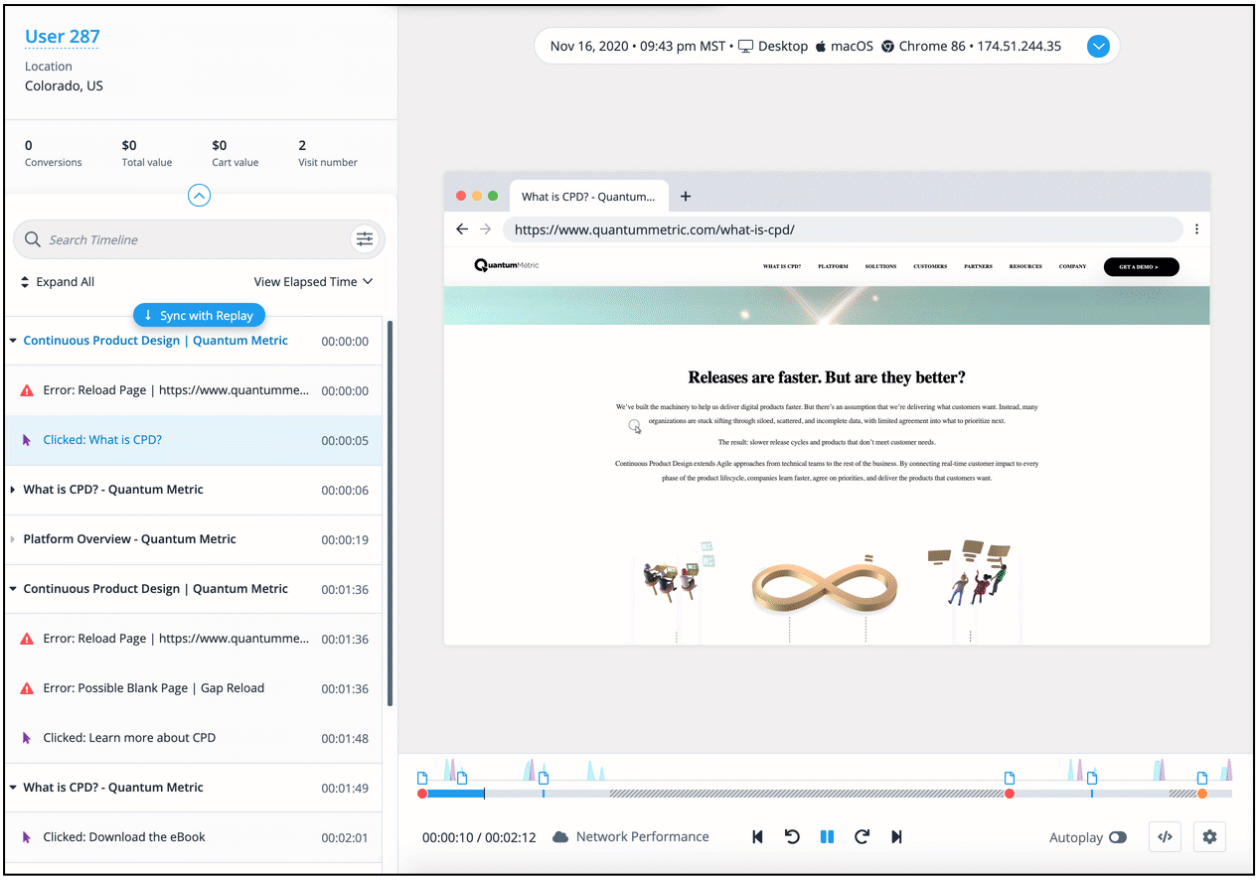


Figure 1

43. The word "replay" is also a bit of a misnomer. The changes to the DOM (*i.e.*, the user's interactions with the website) are captured and transmitted to the session replay provider (*i.e.*, QM) "at hyper-frequent intervals, often just milliseconds apart." *See India Price v. Carnival Corp.*, 712 F.Supp.3d 1347, 1360 (S.D. Cal. Jan. 19, 2024). Thus, the capturing and reading of user information occurs in real time and contemporaneously with the communication.

[6] https://www.quantummetric.com/enterprise-guide-to-session-replay/#h1.

44. QM's patent is illustrative of this contemporaneous interception. When a user communicates with a website (in the form of interactions like clicking items of interest or entering search terms), that information is transmitted to a web server. But, along the way, the "server-side capture engine" (QM's service) intercepts those communications. QM's service also captures communications being sent back from the website to the user[7]:

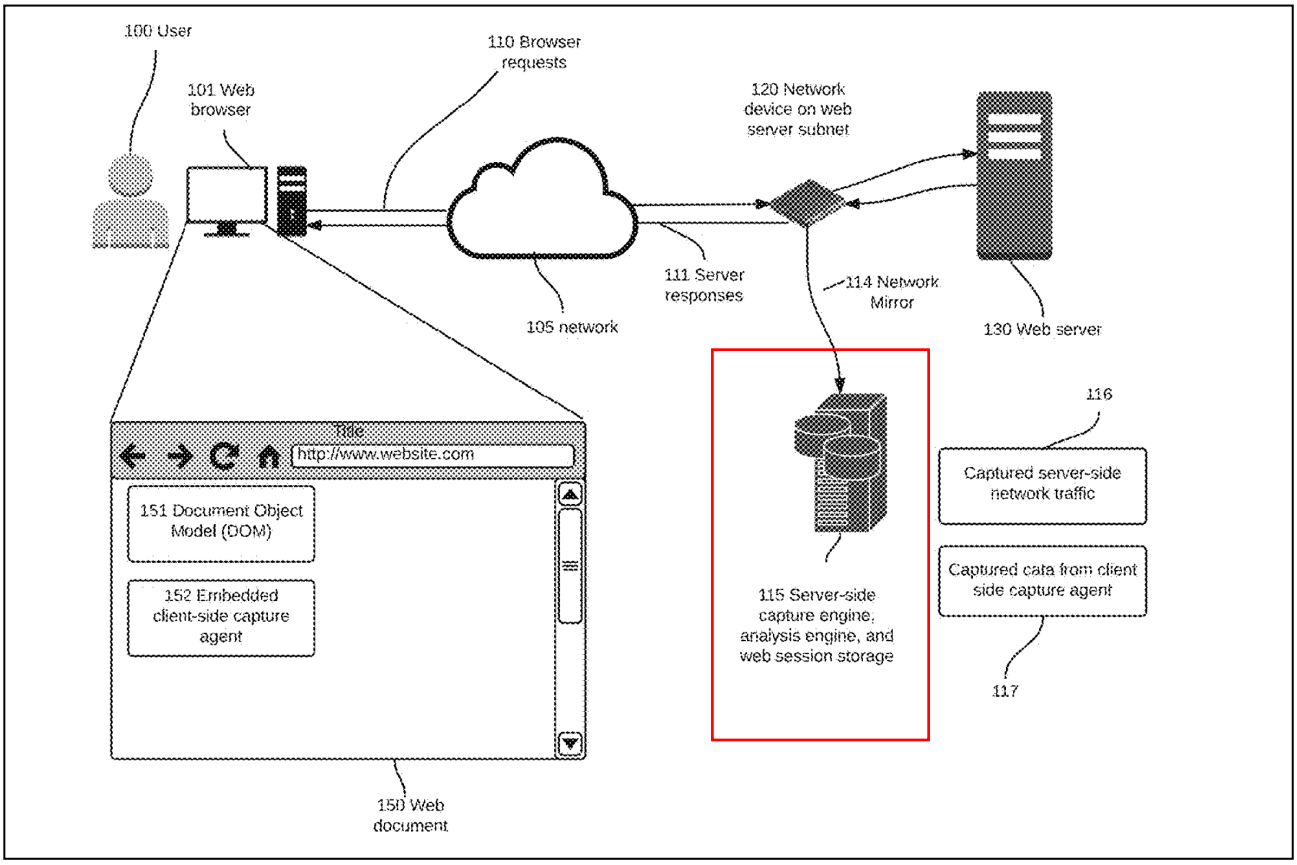


Figure 2

45. Because QM's session replay service operates in the same manner as alleged above, QM's session replay service suffers from the same privacy flaws as its competitors. As an article from the Center for Information Technology Policy at Princeton University found:

> the extent of data collected by these services far exceeds user expectations … text typed into forms is collected before the

[7] *Accurate And Efficient Recording Of User Experience, GUI Changes And User Interaction Events On A Remote Web Document*, U.S. Patent No. 10,146,752, at fig. 1 (issued Dec. 4, 2018).

> user submits the form, and precise mouse movements are saved, all without any visual indication to the user. This data can't reasonably be expected to be kept anonymous.[8]

46. As the article goes on to note, "[c]ollection of page content by third-party replay scripts may cause *sensitive information such as medical conditions*, credit card details and other personal information displayed on a page to leak to the third-party as part of the recording," which "may expose users to identity theft, online scams, and other unwanted behavior."[9]

47. Sensitive user information may be leaked for a multitude of reasons, including but not limited to the fact that (i) "[a]utomated redaction is imperfect; fields are redacted by input element type or heuristics, which may not always match the implementation used by publishers (*e.g.*, information may be redacted when a form field auto-completes, but not when it is manually entered); (ii) page content may not be redacted, even if user inputs are; and (iii) websites operators must manually configure and label personal information to be redacted, which does not always occur."[10]

48. QM is no exception to this. Each mobile app operator must manually select whether information should be captured, not captured, or encrypted.[11] This is an imperfect process. For instance, and as alleged in more detail below, on CVS' Application, consumer PII and the full names of prescription medications are captured unencrypted by QM alongside other information, despite QM's claim that it allegedly "separately encrypt[s]" user PII and "separate[s] any PII data that can be used to re-identify a user, from any analytical data collected."[12]

49. In other words, contrary to its alleged promises, QM intercepted user PII and

---

[8] https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.
[9] *Id.* (emphasis added).
[10] *Id*.
[11] https://www.quantummetric.com/platform/data-privacy-security/.
[12] https://www.quantummetric.com/platform/data-privacy-security.

medical information *unencrypted* and *alongside other information allowing identification*. This is caused by CVS' configuration and implementation of QM's service.

50. In addition to capturing PII and medical information, QM's Session Replay feature captures other identifiers, including a user's IP address:

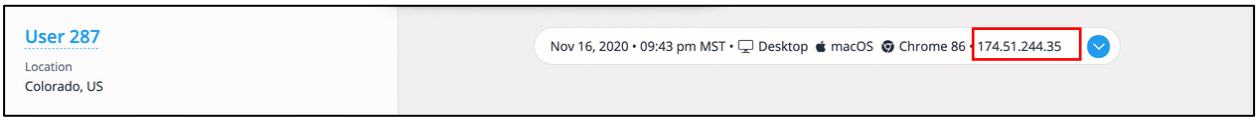


Figure 3

51. An IP address is a unique set of numbers assigned to a device on a network, which is typically expressed as four sets of numbers separated by periods (*e.g.*, 192.168.123.132). The first two sets of numbers indicate what network the device is on (*e.g.*, 192.168), and the second two sets of numbers identify the specific device (*e.g.*, 123.132).

52. Through an IP address, a device's state, city, zip code, and approximate latitude and longitude can be determined. Thus, knowing a user's public IP address—and therefore geographical location—"provide[s] a level of specificity previously unfound in marketing."[13]

53. A public IP address allows advertisers to (i) "[t]arget [customers by] countries, cities, neighborhoods, and … postal code"[14] and (ii) "to target specific households, businesses[,] and even individuals with ads that are relevant to their interests."[15] Indeed, "IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a]

[13] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.
[14] *Location-Based Targeting That Puts You in Control*, CHOOZLE, https://choozle.com/geotargeting-strategies/.
[15] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf.

product or service"[16] because "[c]ompanies can use an IP address … to personally identify individuals."[17]

54. In fact, a public IP address is a common identifier used for "geomarketing," which is "the practice of using location data to identify and serve marketing messages to a highly-targeted audience. Essentially, geomarketing allows [websites] to better serve [their] audience by giving [them] an inside look into where they are, where they have been, and what kinds of products or services will appeal to their needs."[18] For example, for a job fair in specific city, companies can send advertisements to only those in the general location of the upcoming event.[19]

55. "IP targeting is a highly effective digital advertising technique that allows you to deliver ads to specific physical addresses based on their internet protocol (IP) address. IP targeting technology works by matching physical addresses to IP addresses, allowing advertisers to serve ads to specific households or businesses based on their location."[20]

56. "IP targeting capabilities are highly precise, with an accuracy rate of over 95%. This means that advertisers can deliver highly targeted ads to specific households or businesses, rather than relying on more general demographics or behavioral data."[21]

57. In addition to "reach[ing] their target audience with greater precision," businesses

---

[16] *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), https://www.accudata.com/blog/ip-targeting/.
[17] Trey Titone, *The Future Of Ip Address As An Advertising Identifier*, AD TECH EXPLAINED (May 16, 2022), https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/.
[18] *See*, *e.g.*, *The Essential Guide to Geomarketing: Strategies, Tips & More*, DEEP SYNC (Nov. 20, 2023), https://deepsync.com/geomarketing/.
[19] *See*, *e.g.*, *Personalize Your Website And Digital Marketing Using IP Address*, GEOFLI, https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns.
[20] *IP Targeting*, SAVANT DSP, https://www.savantdsp.com/ip-targeting?gad_source=1&gclid=Cj0KCQjw1Yy5BhD-ARIsAI0RbXZJKJSqMI6p1xAxyqai1WhAiXRJTbX8qYhNuEvIfSCJ4jfOV5-5maUaAgtNEALw_wcB.
[21] *Id*.

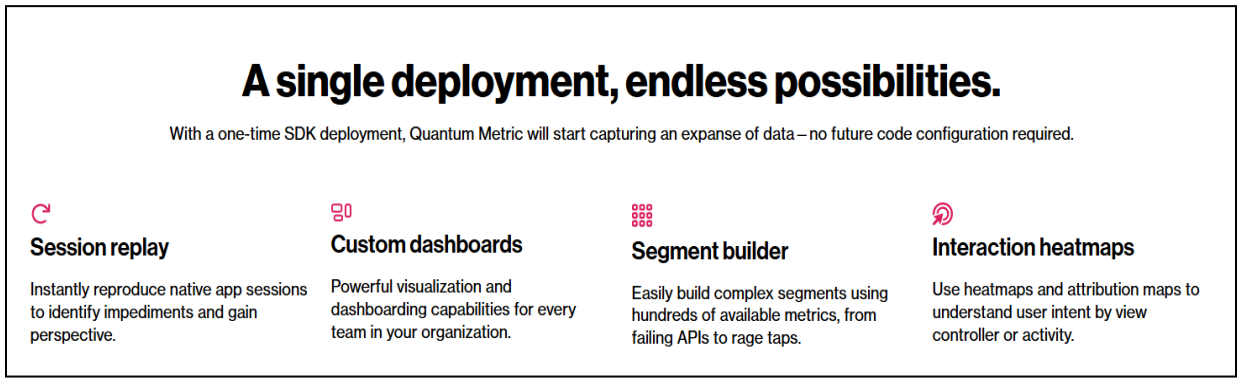
are incentivized to use a customer's public IP address because it "can be more cost-effective than other forms of advertising."[22] "By targeting specific households or businesses, businesses can avoid wasting money on ads that are unlikely to be seen by their target audience."[23]

58. In addition, "IP address targeting can help businesses to improve their overall marketing strategy."[24] "By analyzing data on which households or businesses are responding to their ads, businesses can refine their targeting strategy and improve their overall marketing efforts."[25]

59. For these reasons, under Europe's General Data Protection Regulation, IP addresses are considered "personal data, as they can potentially be used to identify an individual."[26]

2. Data Analytics, AI, And Partner Integrations

60. Beyond capturing and reading a user's personal information, QM also has the capability to analyze the captured information with a sophisticated suite of services—including AI—and further disclose captured user information to other third parties.[27]:



[22] Herbert Williams, *The Benefits of IP Address Targeting for Local Business*es, LINKEDIN (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf.
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] IS AN IP ADDRESS PERSONAL DATA?, CONVESIO, https://convesio.com/knowledgebase/article/is-an-ip-address-personal-data/; *see also* WHAT IS PERSONAL DATA?, EUROPEAN COMMISSION, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en
[27] https://www.quantummetric.com/platform/mobile-app-analytics.

Figure 4

61. QM further advertises that it "will start capturing data out of the box. More than just app crashes – capture behavioral indicators, conversion data points, API performance, and more," as shown on their website[28]:

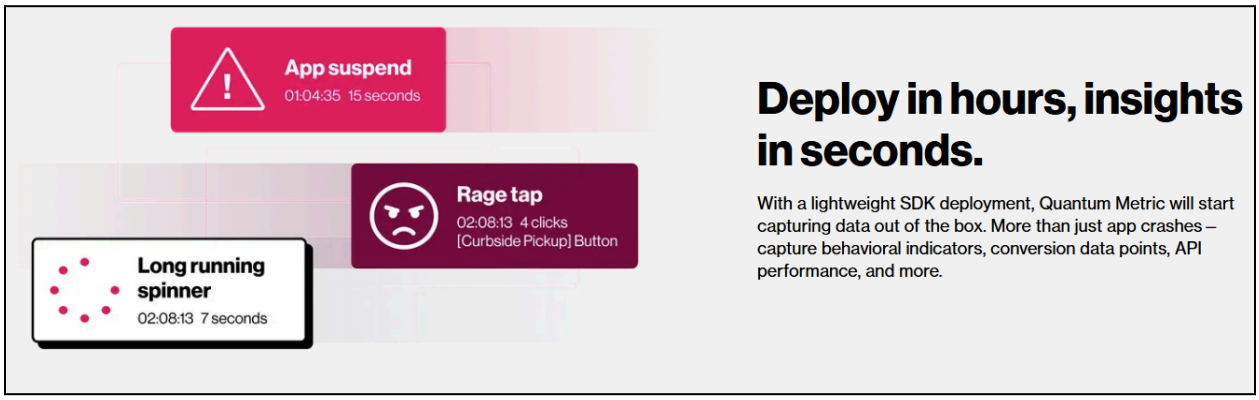


Figure 5

62. QM provides its partners, like CVS, with analytics, including behavioral metrics, technical metrics, and business metrics. Defendant also collects "over 300 audience dimensions such as browser, device type, and location."[29]

63. The behavioral metrics CVS collects includes "clicks, taps, scrolls, long running spinners, scroll depth, form submits, back button usage, page views, typed text, frustration signals, and more."[30]

64. QM's website touts its autocapture feature, telling customers to "leverage the power of Quantum Metric's autocapture for every user interaction – swipe, click, scroll, API response, page view, and more – to enhance and improve its understanding of your data."[31]

65. Moreover, QM's Feliz AI tool has the capacity to "automatically summarize the

[28] *Id.*
[29] https://www.quantummetric.com/platform/data-capture-and-activation/
[30] *Id.*
[31] https://www.quantummetric.com/platform/platform-intelligence/

thousands of data points collected in a user session and consolidates the session timeline into a short, readable summary."[32]

66. QM's services also utilize the assistance of third parties, including but not limited to, Google Analytics, Adobe Analytics, Salesforce, AppDynamics, and more.[33] QM thus shares users' information with these third parties.

67. For example, QM's website explains customers can "enrich Google Analytics with digital experience metrics and deep links into the Quantum Metric platform."[34] This allows customers to receive "enhanced learning" including "a complete overview of every user session."[35] QM provides the same explanation for its use of Adobe Analytics.[36]

68. QM's customers, like CVS, incorporate these services into their mobile applications.

69. Because QM has the capability to "capture[], store[], and interpret[] [] real-time data," it is not like a tape recorder or "tool" used by one party to record another. *See Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021) (finding plaintiff sufficiently alleged QM was akin to "an eavesdropper standing outside the door"). Instead, QM—a separate and distinct third-party entity from the parties to the conversation (Plaintiffs and Class Members, on the one hand, and CVS, on the other)—eavesdrops upon, records, extract data from, and analyzes a conversation to which it was not a party. This is because QM itself is collecting the content of any conversation. That data is then analyzed by QM in the manner alleged above before

[32] *Id.*
[33] https://www.quantummetric.com/partners/partner-network/#technology,customer-experience,performance-monitoring,marketing-analysis,experimentation.
[34] https://www.quantummetric.com/partners/integration-google-analytics/
[35] *Id.*
[36] https://www.quantummetric.com/partners/integration-adobe-analytics/

being provided to any entity that was a party to the conversation (like CVS).

70. QM business model involves providing the services outlined above for a fee to mobile app developers. One of QM's featured clients is CVS:

Figure 6

71. QM operates on CVS' Application in the manner described above. Thus, on CVS' Application, QM captures users' electronic communications in real-time through its Session Replay feature, and then has the capability to analyze those communications and divulge them to other third parties.

72. QM's begins intercepting user information as soon as a user accesses the Application. Thus, users are not on notice of QM's wiretapping, nor do users provide their consent to the same.

B. OVERVIEW OF ADOBE'S TRACKERS

73. Unbeknownst to Plaintiffs and Class Members, CVS also installed code onto the Website that includes a software develop kit ("SDK") offered by Adobe ("Adobe Trackers") associated with the "Adobe Experience Cloud," which allows Adobe to intercept Website users' activity and PHI. The Adobe Trackers intercept and collect a host of Private Information Website users submit, including, *inter alia*:

(a) exact text entered into the search bar on the Website,

(b) over-the-counter drug and prescription drug products that Website users, including patients, searched for, viewed, placed in their shopping cart, or purchased,

(c) appointments patients scheduled to receive vaccinations, including the names of the vaccine(s) and the location and date and time they were to be administered, and

(d) information concerning MinuteClinic appointments, including the symptoms patients were experiencing or the medical procedure they requested and the store zip code.

74. The Adobe Experience Cloud consists of Adobe's integrated online marketing and web analytics products. Although discovery is necessary to confirm the full extent of Adobe Experience Cloud products incorporated onto the Website, the products compromising the various Adobe Trackers installed on the Website are numerous and include, at a minimum: Adobe Analytics, Adobe Launcher, Adobe Advertising Cloud ("everesttech.net"), Adobe Target, Adobe Audience Manger, and the Adobe Experience Cloud Identity Service.

75. Adobe's tracking technology, such as Adobe Analytics and Adobe Experience Cloud, collects and processes Website users' data to facilitate CVS' marketing and advertising efforts. When a user visits the Website, the system assigns a unique identifier to the user and collects behavioral data from them, including page views, interactions, and device-related information. This data is transmitted to Adobe's servers, where it is analyzed and used to build or update user profiles for each of those users. Adobe provides access to these profiles and users' private actions to CVS through its marketing and personalization services.

76. The data CVS transmits to Adobe may also be leveraged for audience targeting, segmentation, and integration with third-party advertising networks. The dangers to personal privacy include the fact that sensitive PHI, including medications and health conditions, are linked to the profiles, exposing Website users to targeted advertising based on their private health choices.

77. CVS' exposure of its customers' data to Adobe's ecosystem without consent violates users' privacy and constitutes misuse by third-party advertisers, and also establishes Adobe's capabilities of transmitting this data to third parties other than CVS for its own commercial benefits, including Meta/Facebook and additional third-party services including Criteo, adsrvr.org/The Trade Desk, and QM. As described below, CVS additionally transmits

Website users' communications directly to Criteo.

78. Specifically, the Adobe Trackers enable Adobe's data collection and sharing via server connections. They operate as tracking scripts and software that intercept and collect a user's internet activity data through multiple user identifiers and cookies. The Adobe Trackers send this information to Adobe-controlled server and/or domains, which host and process data the Adobe Experience Cloud products.

79. The unique user identifiers and cookies Adobe Trackers utilize on the Website include, *inter alia*, those in the following formats: d_mid, demdex, dpm, d_uuid, kndctr_<Org_Id>_AdobeOrg_identity & Id Value, Experience Cloud ID ("d_mid" or "ECID," also known as "MID") (collectively, the "Adobe Identifiers"). Adobe assigns unique values for each of these identifiers for each user, which it uses to track users' activities across devices and accounts. For example, the demdex identifier is a persistent, unique identifier assigned to each visitor on a website or app using Adobe's analytics tools. The demdex ID is stored on a user's browser as a cookie and can be used for tracking and targeting purposes, allowing Adobe to recognize the user on subsequent visits, even if they come from different devices or channels.[37] To help Adobe identify and recognize people across different websites, it uses ID sync parmeter called "d_uuid", which functions as a mapping tag to match Adobe's identifier to third -party IDs. Specifically, the d_uuid appears in web addresses Adobe sends to third-party EverestTech, as described below, to match Adobe's user ID with EverestTech's own ID for the same person. In this way, the d_uuid code helps Adobe Audience Manager and third-parties track Plaintiffs' and

[37] *See* Adobe, Audience Manager Cookies; https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/audience-manager; *see also* Adobe, Cookies and the Experience Cloud Identity Service; https://experienceleague.adobe.com/en/docs/id-service/using/intro/cookies.

Class Members' activity on the Website. In addition, Adobe uses an alphanumeric string to uniquely identify each of its customers across Adobe's products.

80. According to Adobe, "The Experience Cloud ID (MID) [or ECID] is derived mathematically from your organization ID and the demdex ID. As long as these IDs remain constant, generating the right MID for a specific user is simply a math problem. With the same organization ID and demdex ID you get the same MID value, but this depends on the user maintaining the same browser cookies and identifiers. This allows the ID service to track visitors across domains that you control and have configured with ID service code."[38] The Adobe Experience Cloud uses the s_ecid cookie to store a user's ECID and/or MID, and the s_ecid cookie contains a copy of the user's ECID and MID.[39]

81. The ECID, or MID, is a unique user identifier assigned to a specific user that consists of an alphanumeric string, which can be set with Adobe's Experience Cloud Identity Service. It is "a shared identity namespace used across Adobe Experience Platform and Experience Cloud applications to track visitor behavior and ensure that each device has a unique identifier that can persist across multiple sessions."[40] Using the ECID, the Experience Cloud Identity Service:

- "Uniquely identifies a visitor on a device across multiple applications.
- Sets a first-party cookie in customer's domain to ensure tracking on same domain.

  […]
- Receives aliases and ID mappings from Experience Cloud customers and partners.

[38]https://experienceleague.adobe.com/en/docs/id-service/using/intro/cookies#section-15f69c0bac394b4b9966a23fbc586d17
[39]https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/experience-cloud
[40]Adobe, Experience Cloud Identity Service Overview; https://experienceleague.adobe.com/en/docs/id-service/using/intro/overview (accessed July 9, 2025).

- Manages ID synchronization within the Experience Cloud.
- Supports ID synchronization with different third-parties cross the ad tech ecosystem."[41]

82. Adobe uses the ECID to track users across multiple devices and touchpoints, which cross-channel tracking allows it to correlate all actions a user takes, providing a single unified view of the customer's online activity. Adobe visualizes this with the following identity graph:[42]

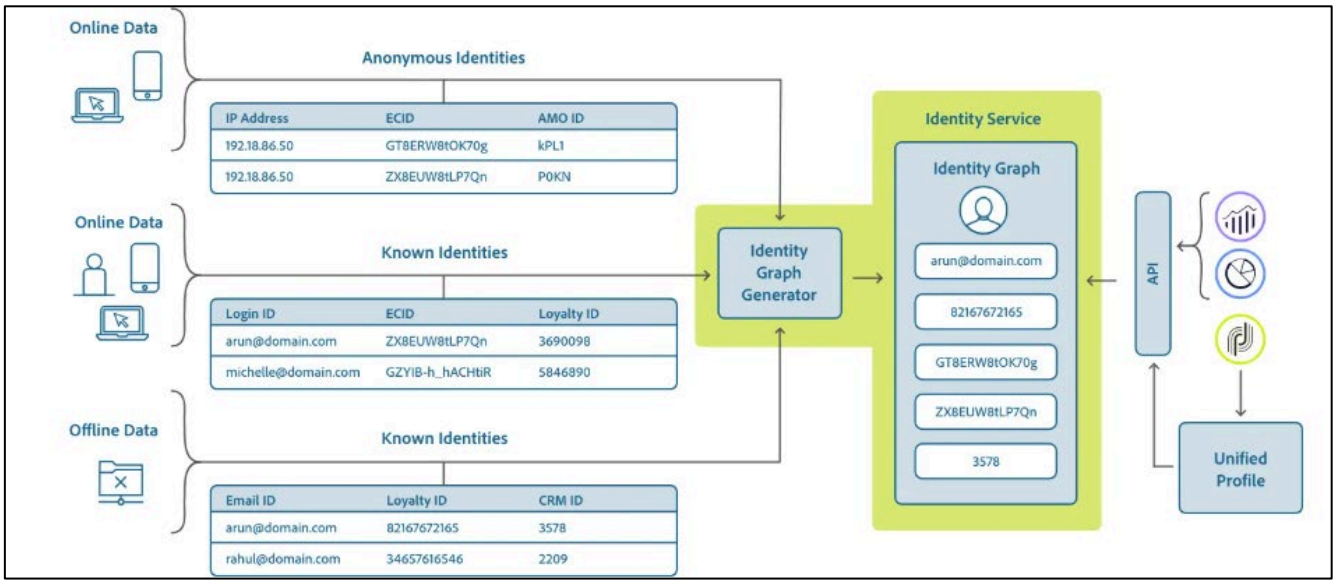


Figure 6

83. Even if users clear cookies, Adobe collects device fingerprinting data (such as tracking browser type, screen resolution, and IP address, etc.), which can help its tracking methods recognize returning users.

84. Meanwhile, Adobe's Demdex server also synchronizes users' unique identifiers with third-party advertising partners like Criteo, EverestTech, and Adsrvr/The Trade Desk,

[41] *Id*.
[42] Adobe, Adobe Experience Platform Identity Service; https://experienceleague.adobe.com/en/docs/experience-platform/identity/home (accessed July 9, 2025).

ensuring that even non-logged-in users see targeted ads based on their browsing behavior.

85. The Demdex IDs are tied to users' activity across different websites that use the Adobe Experience Cloud suite of products, permitting Adobe to track Website users' activity on unrelated websites. In this way, as part of the services Adobe offers to its clients, it incorporates personal data it obtains from users' activity on the Website and across these other, unrelated websites, to serve its customers using a comprehensive profile of the Website user, including the user's Private Information, to enrich its customers' marketing analytics.

86. For example, when a user visits the Website, the Adobe Trackers download a script onto the user's browser. When executed, these scripts disclose Website users' unique Demdex IDs to Adobe-owned servers, including those operated by Adobe's data management platform (DMP). After receiving the users' Demdex ID, Adobe facilitates the setting of an Everest Technologies cookie on the user's browser through a tracking mechanism.

87. Adobe uses Everest Technologies to perform real-time advertising bidding and audience segmentation to enhance advertising display campaigns for its Adobe Experience Cloud customers. Website users' unique Demdex IDs are transmitted to Everest Technologies via Adobe's data-sharing infrastructure when Website users visit the Website. Adobe leverages the personal data that Everest Technologies collects from Website users' activity to provide advertising services for its Adobe Experience Cloud customers. By doing so, Adobe discloses identifiable browsing behavior and associated data points it obtains from Website users' activity to third parties.

88. That Everest Technologies, which operates within Adobe's programmatic advertising ecosystem, obtains Website users' unique Demdex IDs when they visit the Website confirms Adobe's capability to use Website users' behavioral data for its own purposes, including

enhancing targeted advertising strategies for its third-party customers.

89. Indeed, the Adobe Experience Cloud Terms of Use suggest Adobe uses intercepted data for its own operating and marketing services and to improve its services to customers. The terms state: "You grant Adobe a worldwide, royalty-free, non-exclusive, transferable, and sublicensable license to adapt, display, distribute, modify, perform, publish, reproduce, translate, and use Your Materials for the purpose of operating, marketing and improving the Services and enabling your use of the Services."[43] Adobe defines Materials to include the intercepted information at issue here: 'Materials' means any materials provided by You, Adobe, or a third party, including without limitation any (a) user material, including usage and telemetry activities; (b) reports, text, code, data, documents, images, photographs, graphics, audio, videos, or webcasts; (c) products; or (d) Software."[44]

C. CVS ENABLED QM'S WIRETAPPING OF PLAINTIFFS' ELECTRONIC COMMUNICATIONS VIA THE APPLICATION.

90. In October 2024, Plaintiffs' counsel retained a private research company to review and conduct a dynamic analysis on the Application. A "dynamic analysis" records the transmissions that occur from a user's device.

91. The private researchers tested what information (if any) is transmitted to third parties when a user accesses and uses the CVS Application, including when a user is signed into their pharmacy account and refills a prescription and/or purchases or looks at over-the-counter products.

92. The researchers found that on both the Android and iOS mobile applications, when

[43] Adobe, Adobe Experience Cloud Terms of Use https://www.adobe.com/content/dam/cc/en/legal/servicetou/Experience_Cloud_TOU_en_WW_20220608.pdf.
[44] *Id*.

a user is signed into their CVS account, QM—as enabled by CVS—intercepts sensitive medical information alongside PII, allowing QM to identify which individuals are receiving which specific medical treatments.

93. For instance, just when shopping for over-the-counter products, QM intercepts an iOS Application user's first name, e-mail address, the medication they viewed, and their vaccination history when the user is signed into a CVS pharmacy account:

THIRD PARTY	PRODUCT INFO	PERSONAL INFO	OTHER INFO
Quantum Metric	Vaccination History, Viewed Medication	Email, First Name	-

Figure 7

94. In addition, when an Android Application user goes to refill a medication or views their prescription history, QM intercepts their full name, e-mail address, phone number, shipping address, the medication they viewed, their vaccination history, and even the address of the store they fill their prescriptions at:

THIRD PARTY	PRODUCT INFO	PERSONAL INFO	OTHER INFO
Quantum Metric	Store Address, Product Name, Product Price. Product Quantity, Vaccination History, Viewed Medication	Email, Phone Number, First Name, Last Name, Shipping Address	-

Figure 8

95. Crucially, none of this information is encrypted by QM (although it has been redacted by Plaintiffs in the screenshots below to protect the user's privacy). For instance, in the below screenshot from the dynamic analysis of the Android Application, the user's phone number (redacted by Plaintiffs to XXX-XXX-XXXX) and e-mail address (redacted by Plaintiffs to

j[redacted for privacy]@duck.com) were intercepted by QM:

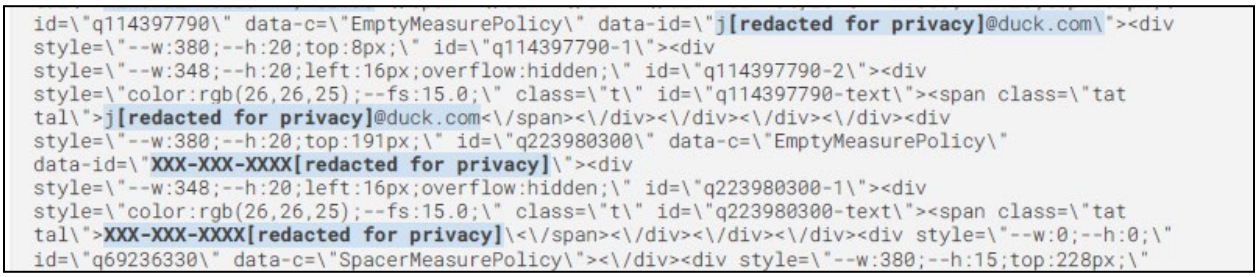


Figure 9

96. In another portion of the same transmission, the user's full name (redacted by Plaintiffs to J[redacted for privacy]) is listed right next to their filled medication, Escitalopram, which is the generic for Lexapro, an anti-depressant:

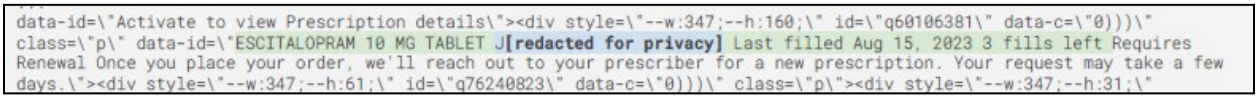


Figure 10

97. And in yet another portion of the same transmission, the user's full name is listed right next to the user's vaccination history:

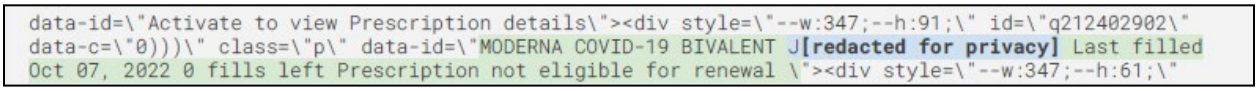


Figure 11

98. QM's wiretapping of Plaintiffs' and Class Members' electronic communications began the moment they accessed the Application and happened in real time. Further, the information QM intercepts is the result of a user interacting with the Application (*e.g.*, filling prescriptions, clicking on items of interest, typing in products into the search field) rather than automatically generated. Thus, QM is intercepting the "contents" of users' affirmative communications with the Application.

99. Neither CVS nor QM asked Plaintiffs and Class Members whether they consented to being wiretapped by QM. Plaintiffs were never explicitly told that their electronic communications were being wiretapped by QM, nor did CVS or QM obtain Plaintiffs' prior

consent to the wiretapping.

100. QM had access to Plaintiffs' and Class Members' communications because QM contracted with CVS to provide its services on the Application.

101. CVS' enabling of QM's wiretapping of consumer Private Information is a massive breach of consumer privacy.

D. CVS ENABLED ADOBE TRACKERS' WIRETAPPING OF PLAINTIFFS' ELECTRONIC COMMUNICATIONS VIA THE WEBSITE.

102. The Adobe Trackers CVS installed on the Website intercept, collect, use, and disclose to third parties Website users' Private Information, and they do so without the Website users' knowledge or consent.

103. Specifically, the Adobe Trackers implemented on the Website intercepted users' activity in at least the following instances: 1) keyword searches, including for over the counter medication and other health products, including sexual health products; 2) viewing, clicking on, and purchasing these healthcare products; 3) selecting vaccines and scheduling appointments for their administration; 4) scheduling MinuteClinic appointments, including the symptoms patients were experiencing or the medical procedure they requested and the store's zip code; and 5) managing prescription drugs.

1. Keyword Searches

104. The Website's homepage encourages users to "search products and services" via its prominently displayed search bar at the top of the page.[45] Patients may run any searches on the Website, regardless of which products CVS stocks. For example, as depicted in Figure 12, below, Website users may search for "aspirin." Indeed, Website users may type an endless variety of

[45] CVS; https://www.cvs.com/

search terms based on their healthcare needs to find sensitive healthcare products that CVS stocks, such as "birth control"[46], "pregnancy tests"[47], "fertility tests"[48], "baby gender DNA tests"[49], and "paternity tests."[50]

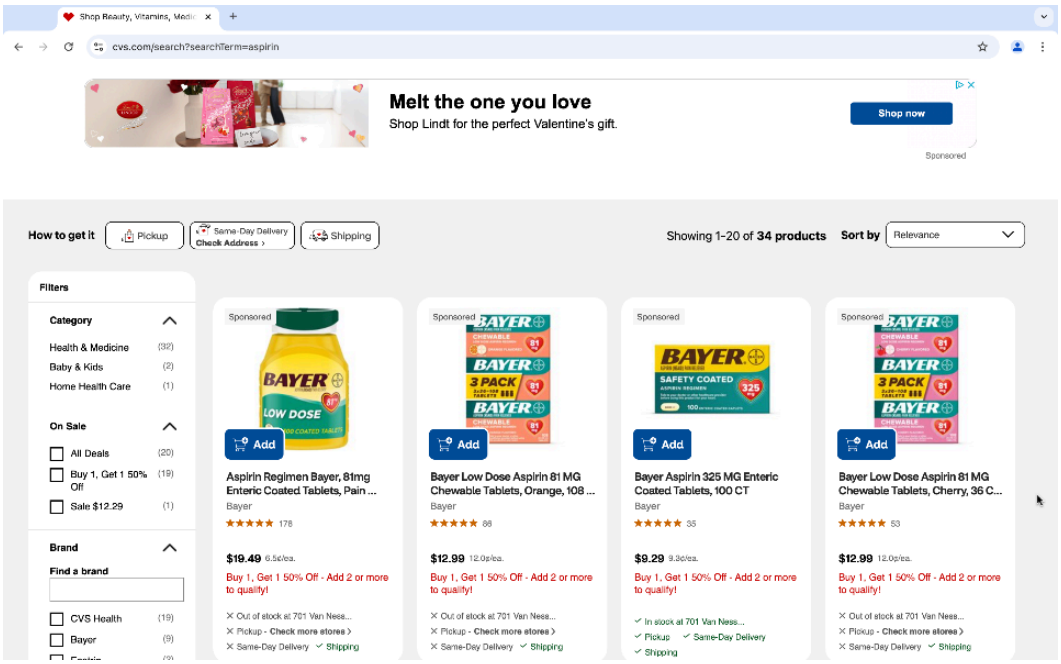


Figure 12

105. As shown in the redacted website traffic between the Website and Adobe's Adobedc.net server in Figure 13, below, which corresponds with the web image displayed in Figure 12, the Adobe Trackers, as implemented by CVS, intercept Website users' Private Information, including any search terms Website users' search via the search bar, unbeknownst to them. Highlighted in yellow, the Adobe Trackers transmitted to Adobe the exact URL of the search results, which expressly includes the search terms: here, "aspirin." Highlighted in blue, the Adobe Tracker also transmits to Adobe each of the search results for the search query, including the

[46] CVS; https://www.cvs.com/search?searchTerm=birth%20control
[47] CVS; https://www.cvs.com/search?searchTerm=pregnancy%20test
[48] CVS; https://www.cvs.com/search?searchTerm=fertility%20test
[49] CVS; https://www.cvs.com/search?searchTerm=baby%20gender%20test
[50] CVS; https://www.cvs.com/search?searchTerm=paternity%20tests

product names, the skuID numbers, and the parentSku numbers. Regardless of the search or search results, the Adobe Tracker is programmed to systematically intercept the search results URL, which include the searches run by Website users, and any products responsive to that search request. Additionally, highlighted in purple, the Adobe Tracker also assigns and tracks unique identifiers assigned to Website users and their activity.

POST https://edge.adobedc.net/ee/or2/v1/interact?configId=1e24809d-8a88-43c9-ba9a-0babf0fb08c7&[redacted] HTTP/2 content-length: 4154 cache-control: max-age=0 sec-ch-ua-platform: “macOS” user-agent: Mozilla/5.0 [redacted] sec-ch-ua: “Not A(Brand”;v=”8”, “Chromium”;v=”132”, “Google Chrome”;v=”132” content-type: text/plain; charset=UTF-8 sec-ch-ua-mobile: ?0 accept: */* origin: https://www.cvs.com sec-fetch-site: cross-site sec-fetch-mode: cors sec-fetch-dest: empty 28ealium28: https://www.cvs.com/search?searchTerm=aspirin accept-encoding: gzip, deflate, br, zstd accept-language: en-US,en;q=0.9 priority: u=1, i host: edge.adobedc.net
{“meta”:{“configOverrides”:{},”sdkConfig”:{“datastream”:{“original”:”2612b8ac-d4b2-4d6d-8d99-878e3f9e5846”}},”state”:{“domain”:”cvs.com”,”cookiesEnabled”:true,”entries”:[{“key”:”kndctr_06660D1556E030D17F000101_AdobeOrg_cluster","value":"or2"},{“key”:”kndctr_06660D1556E030D17F000101_AdobeOrg_Identity","value":"”[redacted]I=”}]}},”events”:[{“query”:{“personalization”:{“schemas”:[“https://ns.adobe.com/personalization/default-content-item”,”https://ns.adobe.com/personalization/html-content-item”,”https://ns.adobe.com/personalization/json-content-item”,”https://ns.adobe.com/personalization/redirect-item”,”https://ns.adobe.com/personalization/ruleset-item”,”https://ns.adobe.com/personalization/message/in-app”,”https://ns.adobe.com/personalization/message/feed-item”,”https://ns.adobe.com/personalization/dom-action”],”decisionScopes”:[“__view__”],”surfaces”:[“web://www.cvs.com/search”]}},”xdm”:{“web”:{“webPageDetails”:{“URL”:”https://www.cvs.com/search?searchTerm=aspirin”},”webReferrer”:{“URL”:”https://www.cvs.com/”},”type”:”other”,”webInteraction”:{“URL”:”https://www.cvs.com/search?searchTerm=aspirin”,”linkClicks”:{“value”:1},”name”:”28ealiu_tracking”}},”device”:{“screenHeight”:982,”screenWidth”:1512,”screenOrientation”:”landscape”},”environment”:{“type”:”browser”,”browserDetails”:{“viewportWidth”:1512,”viewportHeight”:857}},”placeContext”:{“localTimezoneOffset”:-60,”localTime”:”2025-01-31T08:59:07.324+01:00”},”timestamp”:”[redacted]”,”implementationDetails”:{“name”:”https://ns.adobe.com/experience/alloy","version":"2.19.2","environment”:”browser”},”eventType”:”web.cmxImpressionTracking.linkClic”s”,"_cvs":{”Criteo”:{“criteoCustomerID”:””,”criteoVisitorID”:”1738310345737”,”criteoProductDetails”:[{“clientAdvertiserId”:”7915838","productName”:”Bayer Aspirin 81mg Low Dose Enteric Coated Tablets”,”skuID”:”126928”,”parentSku”:”1012177”,”productPosition”:”28ealiu”,”criteoOnLoad”:”1”},{“clientAdvertiserId”:”7915838”,”productName”:”BAYER RAPID RELIEF RASPBERRY POWDER PACKS”,”skuID”:”181185”,”parentSku”:”7200047”,”productPosition”:”28ealiu”,”criteoOnLoad”:”1”},{“clientAdvertiserId”:”7915838”,”productName”:”Bayer Back&Body

Aspirin500mg+Caff32.5mg X-Str Coated Caplets”,”skuID”:”207980”,”parentSku”:”1012207”,”productPosition”:”29ealiu”,”criteoOnLoad”:”1”},{“clientAdvertiserId”:”7868529”,”productName”:”EXCEDRIN TENSION HEADACHE CAPLETS”,”skuID”:”265984”,”parentSku”:”265984”,”productPosition”:”29ealiu”,”criteoOnLoad”:”1”},{“clientAdvertiserId”:”7915838”,”productName”:”BAYER LOW DOSE ASPIRIN CHERRY 81MG CHEWABLE TABLETS 3PK”,”skuID”:”298486”,”parentSku”:”298486",”productPosition”:”29ealiu”,”criteoOnLoad”:”1”},{“clientAdvertiserId”:”7915838","productName":"Bayer Aspirin 81mg Low Dose Chewable Tablets Orange Flavored”,”skuID”:”522987”,”parentSku”:"522987”,”productPosition”:”29ealiu”,”criteoOnLoad”:”1”},{“clientAdvertiserId”:”7915838”,”productName”:”BAYER ASPIRIN SAFETY COATED 325MG CAPLETS 100CT”,”skuID”:”669317”,”parentSku”:”1012106”,”productPosition”:”29ealiu”,”criteoOnLoad”:”1”},{“clientAdvertiserId”:”7915838”,”productName”:”Bayer Aspirin 81mg Low Dose Enteric Coated Tablets”,”skuID”:”695200”,”parentSku”:”1012066”,”productPosition”:”29ealiu”,”criteoOnLoad”:”1”},{“clientAdvertiserId”:”7915838”,”productName”:”Bayer Aspirin 325mg Coated Tablets”,”skuID”:”695201”,”parentSku”:”1012212”,”productPosition”:”29ealiu”,”criteoOnLoad”:”1”},{“clientAdvertiserId”:”7868529”,”productName”:”Excedrin Migraine Acet250mg+Asprn250mg+Caff65mg X-Str Caplet”,”skuID”:”906001”,”parentSku”:”1012028”,”productPosition”:”29ealiu”,”criteoOnLoad”:”1”},{“clientAdvertiserId”:”7868529”,”productName”:”Excedrin Extra Strength Acet250mg+Asprn250mg+Caff65mg Caplet”,”skuID”:”917967”,”parentSku”:”1012217”,”productPosition”:”29ealiu”,”criteoOnLoad”:”1”},{“clientAdvertiserId”:”7915838”,”productName”:”Bayer Aspirin 81mg Low Dose Chewable Tablets Orange Flavored”,”skuID”:”947994”,”parentSku”:"947994",”productPosition”:”29ealiu”,”criteoOnLoad”:”1”}]},”29ealium_cmx_event”:"criteo_on_pag”_”oad",”c”xTimeS”a”p”:”1738310347281”}}}],”query”:{“identity”:{“fetch”:[“ECID”]}}}

Figure 13

106. The web image and code depicted in Figure 12 and Figure 13 reflect the activities of Website users who are proceeding as guests. However, the Adobe Trackers intercept the same substantive information reflected in these figures when a Website user is logged in, except that, when logged in, Adobe also intercepts additional persistent user identifiers, such as a PPID, which CVS transmits to allow Adobe to recognize logged in users and associate the user's behavior across visits.

107. Additionally, while discovery is required to confirm the full extent of Private Information exchanged between Adobe and Criteo, upon information and belief, Adobe shares information it intercepts with Criteo, including but not limited to these keyword searches and

unique identifiers, permitting Criteo to further enhance its own customer profiles by synchronizing and cross referencing Criteo's data with information Adobe collects and stores in its ad ecosystem.

2. Viewing, clicking on, and purchasing medicine and merchandise

108. After searching for products, including medicine, over the counter drugs, and other healthcare products, Website users may click on the products, place them in their shopping cart, and proceed to the checkout screen for purchase with those products in their cart. Figures 14 and 15 below, as redacted, show a user who has proceeded to the checkout screen with the following product in the user's shopping cart: Aspirin Regimen Bayer, 81mg Enteric Coated Tablets, Pain Reliever/Fever Reducer, 300 ct.[51]

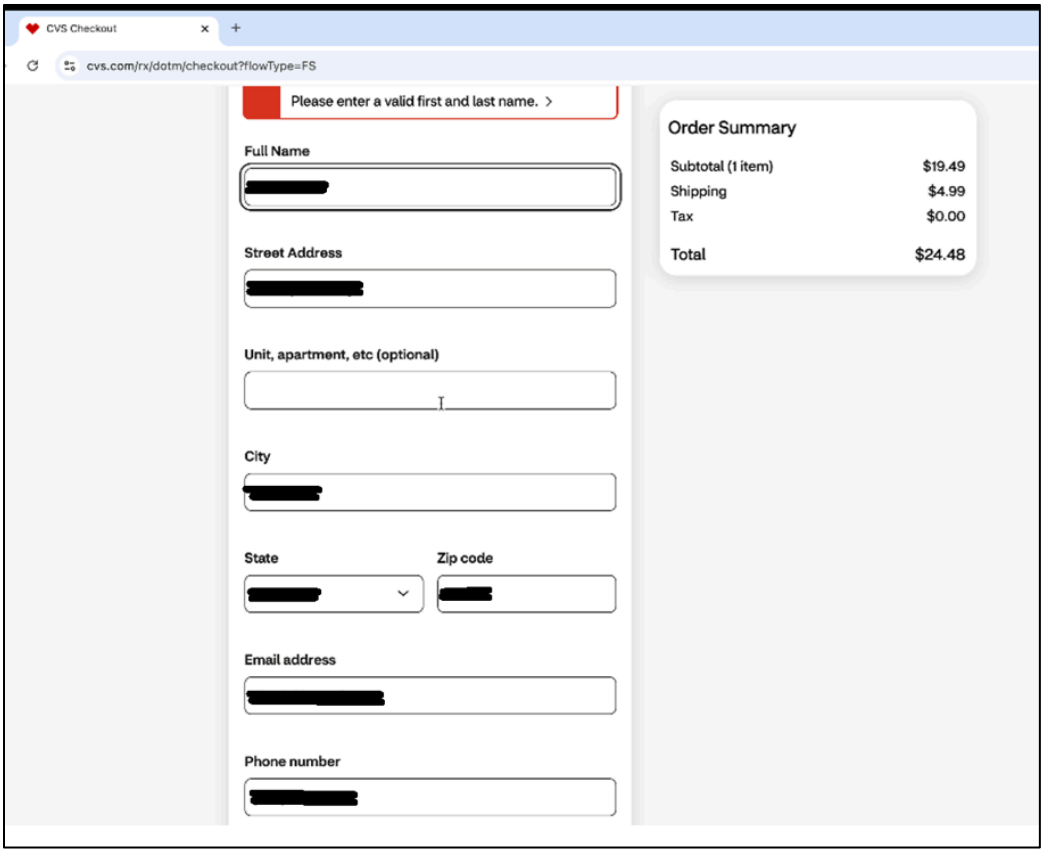


Figure 14

[51] *See* https://www.cvs.com/shop/aspirin-regimen-bayer-81mg-enteric-coated-tablets-pain-reliever-fever-reducer-300-ct-prodid-1012066

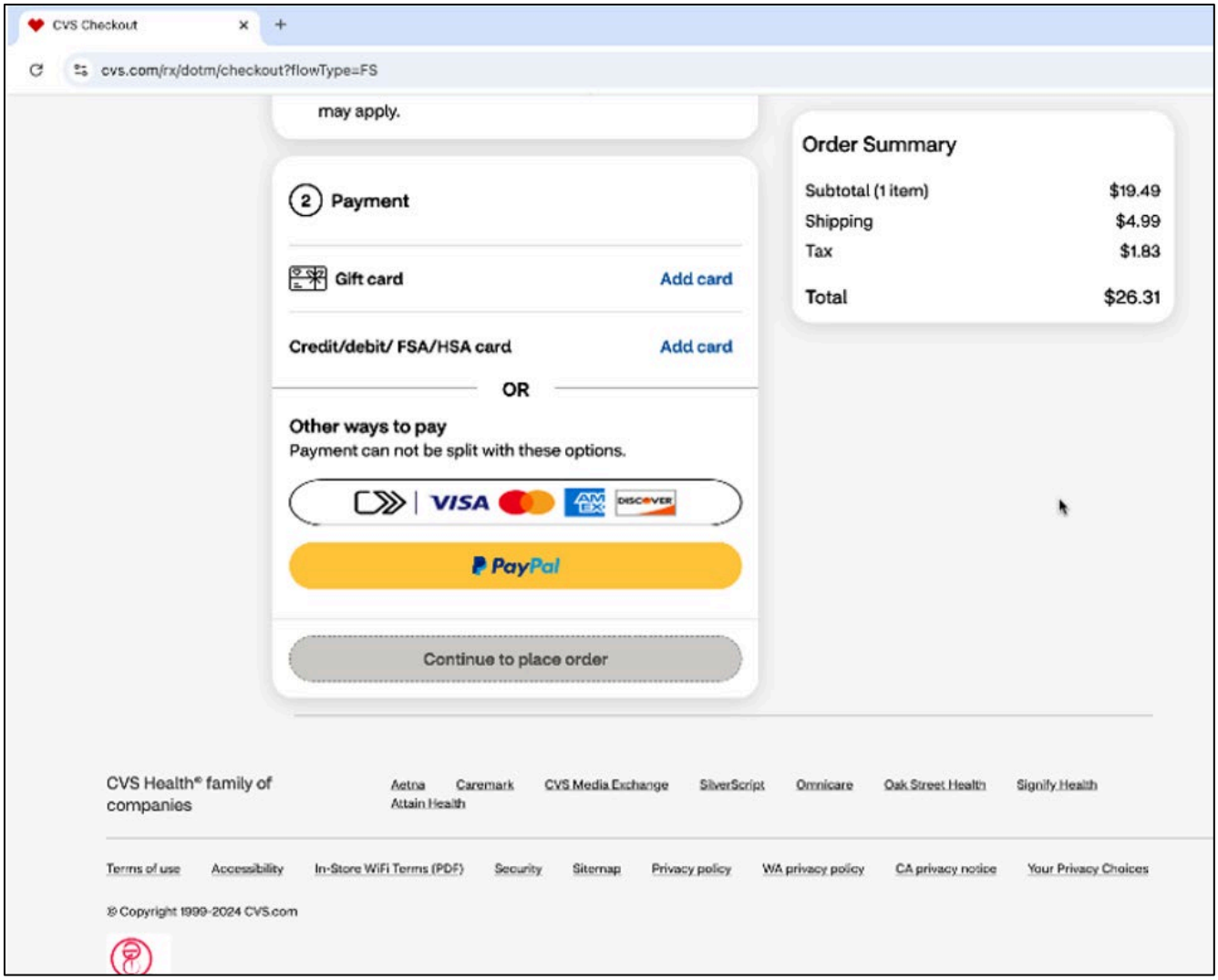


Figure 15

109. Moreover, as shown in the redacted website traffic between the Website and Adobe's Adobedc.net server in Figure 16, below, which corresponds with the web image displayed in Figures 14 and 15, the Adobe Trackers, as created and facilitated by Adobe and implemented by CVS, capture and transmit user's browsing and transactional data, including searches. Highlighted in yellow, the Adobe Trackers transmit to Adobe both the URL of the checkout page, disclosing that the Website user is purchasing the product in his cart, and the URL of the product, together with the product ID, disclosing the exact identity of the purchased product.

110. Highlighted in blue, the Adobe Tracker also tracks the purchase event. The

"MetaConversion_Purchase" event is a type of event Adobe's Experience Cloud uses to record and track purchases or conversions made by a user on a website, and the "metaActionSource," "metaTimeStamp," and "metaCurrencyCode" track additional details of the conversion or purchase and disclose them to third-party Meta: in this instance, that the purchase was made via a website, the date and time, and that the purchase is being made on a website. Additionally, the "metaFBP" event stands for Facebook Pixel, which refers to the Facebook First-Party Cookie ID, used by Meta's Facebook Pixel to track user interactions on the website and link them to advertising campaigns on Meta's platforms. The value fb.1.173[redacted]0 consists of the Facebook Pixel prefix (fb.1), a timestamp ([redacted]), and a unique session identifier (8[redacted]0), which together allow Facebook to associate the user's session with advertising and tracking data.

111. Through CVS' use of Adobe's event trackers (like MetaConversion_Purchase), Adobe collects Facebook-related data, such as the Facebook Pixel ID (metaFBP), which is a unique identifier tied to a user's browser session. This allows Adobe and Defendants, CVS, Criteo, and Medallia, to track user actions (e.g., purchases) and correlate them with Facebook ad interactions for attribution and retargeting purposes.

112. Regardless of the product Website users purchase, the Adobe Tracker is programmed to systematically intercept and disclose the same information. Additionally, highlighted in purple, the Adobe Tracker also assigns and tracks unique identifiers assigned to Website users and their activity on the Website, which are used, as described above, to individually identify the Website user.

113. The web images and traffic depicted in Figures 14, 15, and 16 reflect the activities of Website users proceeding as guests. However, the Adobe Trackers intercept the same

substantive information reflected in these figures when a Website user is logged in, except that, when logged in, Adobe also intercepts additional persistent user identifiers, such as a PPID, which CVS transmits to allow Adobe to recognize logged in users and associate the user's behavior across visits.

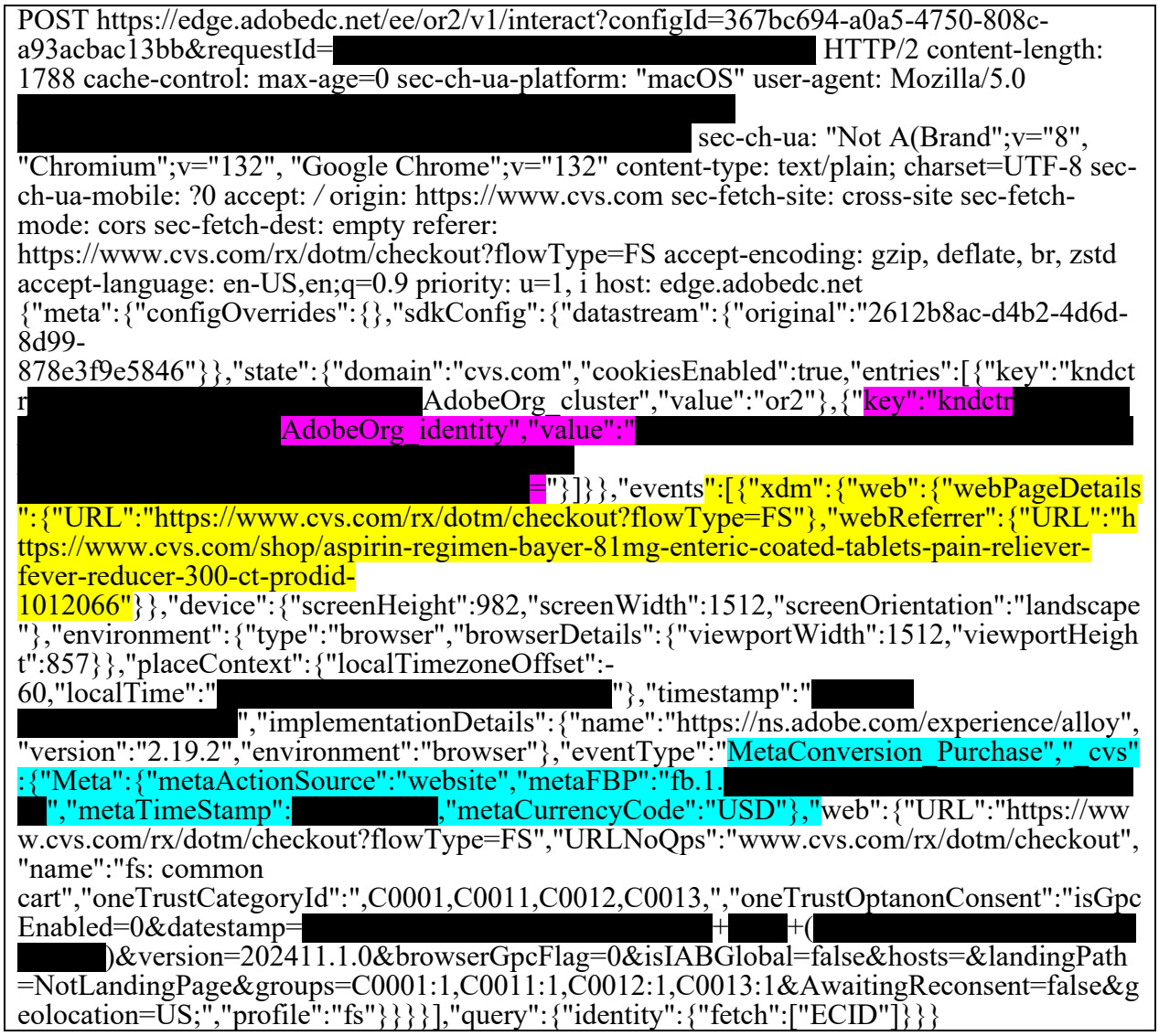


Figure 16

114. Similarly, regardless of whether the Website user is logged in or proceeding as a guest, the Adobe Trackers also intercept the "productName"—in this case, Bayer Aspirin 81mg Low Dose Chewable Tablets Orange Flavored—and the "SkuID" and "parentSku"—in this case,

947994—to identify any products that a Website user clicks on that are responsive to searches to the user runs. As with purchases, Adobe also discloses to Meta when Website users click on these products, as evidenced by the following web traffic:

> MetaConversion_PageView","_cvs":{"Meta":{"metaActionSource":"website","metaEventID":"2960655307021616","metaFBP":"fb.1.1738310305172.[redacted]","metaTimeStamp":[redacted]},"web":{"**URL":"https://www.cvs.com/shop/aspirin-regimen-bayer-81mg-enteric-coated-tablets-pain-reliever-fever-reducer-300-ct-prodid-1012066**","URLNoQps":"www.cvs.com/shop/aspirin-regimen-bayer-81mg-enteric-coated-tablets-pain-reliever-fever-reducer-300-ct-prodid-1012066","name":"shop:pdp:Aspirin Regimen Bayer, 81mg Enteric Coated Tablets, Pain Reliever/Fever Reducer, 300 ct(695200)"

115. Likewise, and also regardless of whether the Website user is logged in or proceeding as a guest, the Adobe Trackers also intercept the identity of the product whenever a Website user places them in their cart, including by intercepting the reference URL of the product and the product SKU, as set forth in the following web traffic excerpt:

> “decisionScopes”:[“__view__”],”surfaces”:[“web://www.cvs.com/rx/dotm/cart”]}},”xdm”:{“web”:{“webPageDetails”:{“URL”:”https://www.cvs.com/rx/dotm/cart?flowType=FS”,”pageViews”:{“value”:1},”name”:”cvs|dweb|rx|dotm|cart|fs: common cart”},”**webReferrer”:{“URL”:”https://www.cvs.com/shop/aspirin-regimen-bayer-81mg-enteric-coated-tablets-pain-reliever-fever-reducer-300-ct-prodid-1012066”}}**
>
> […]
>
> “,”prop23”:”www.cvs.com/rx/dotm/cart”,”prop46”:”sl_v2=|slsdp=“},”lists”:{“list3”:{“list”:[{“value”:”cs:Get_everything_you_need”}]}}},”event1to100”:{“event45”:{“value”:1}},”event101to200”:{“event107”:{“value”:0}},”event201to300”:{“event269”:{“value”:24.48}},”event301to400”:{}}},”productListItems”:[{“SKU”:”695200”,”_experience”:{“analytics”:{“customDimensions”:{“eVars”:{“eVar47”:”fs”,”eVar71”:”695200”,”eVar174”:”false”}},”event101to200”:{“event170”:{“value”:1}},”event201to300”:{}}}}],”commerce”:{“productListViews”:{“value”:1}}},”data”:{“productstring”:”;695200;;;event170;eVar47=fs|eVar71=695200
>
> […]

3. Scheduling Vaccinations

116. The Website also invites Website users to select vaccines and schedule appointments for their administration. As depicted below in Figures 17A, 17B, and 17C, as redacted, after selecting vaccines for administration and entering additional information, the Website requires users to confirm information they submitted, including their name, email address, phone number, the name of the vaccines, and the date, time, and location of the appointment.

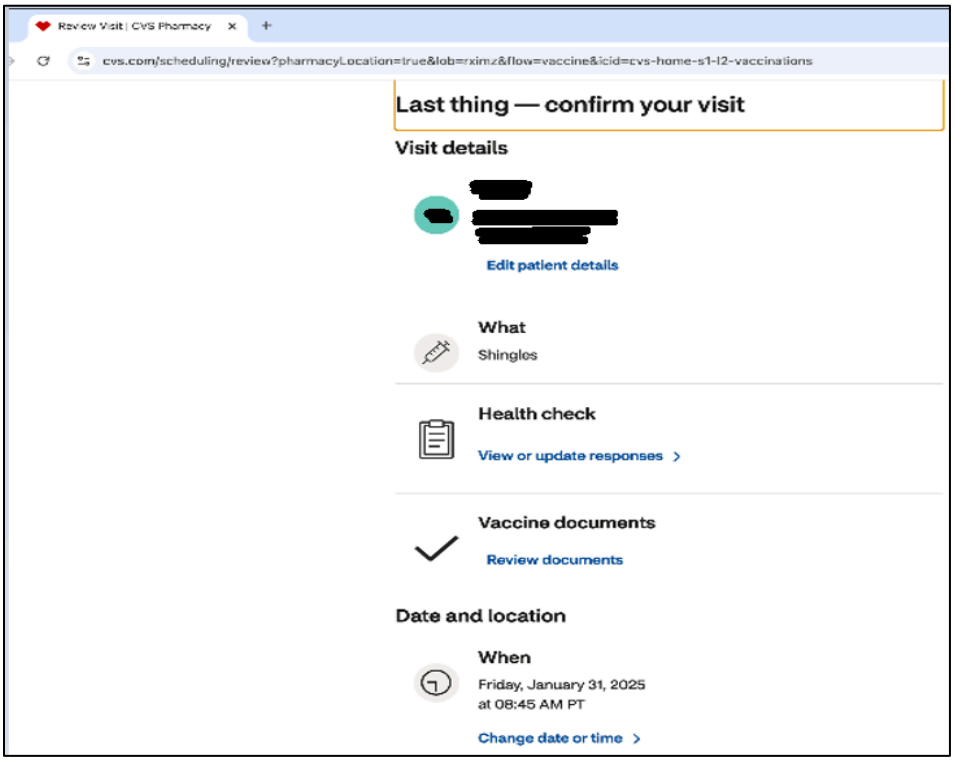


Figure 17A

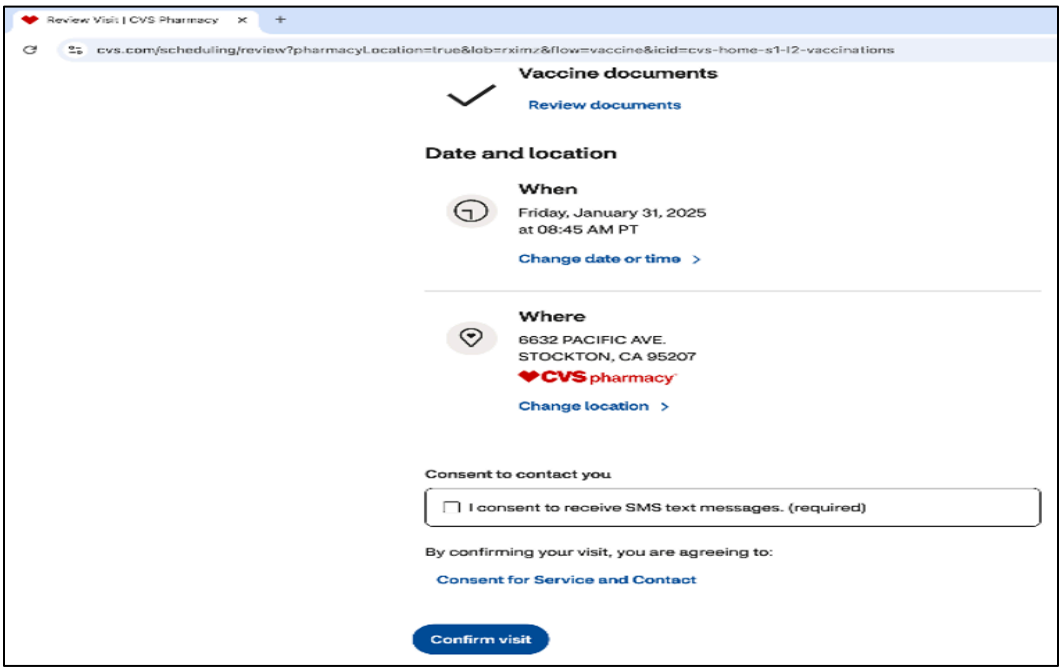

Review Visit | CVS Pharmacy
cvs.com/scheduling/review?pharmacyLocation=true&lob=rximz&flow=vaccine&icid=cvs-home-s1-l2-vaccinations
Vaccine documents
Review documents
Date and location
When
Friday, January 31, 2025
at 08:45 AM PT
Change date or time >
Where
6632 PACIFIC AVE.
STOCKTON, CA 95207
CVS pharmacy
Change location >
Consent to contact you
I consent to receive SMS text messages. (required)
By confirming your visit, you are agreeing to:
Consent for Service and Contact
Confirm visit

Figure 17B

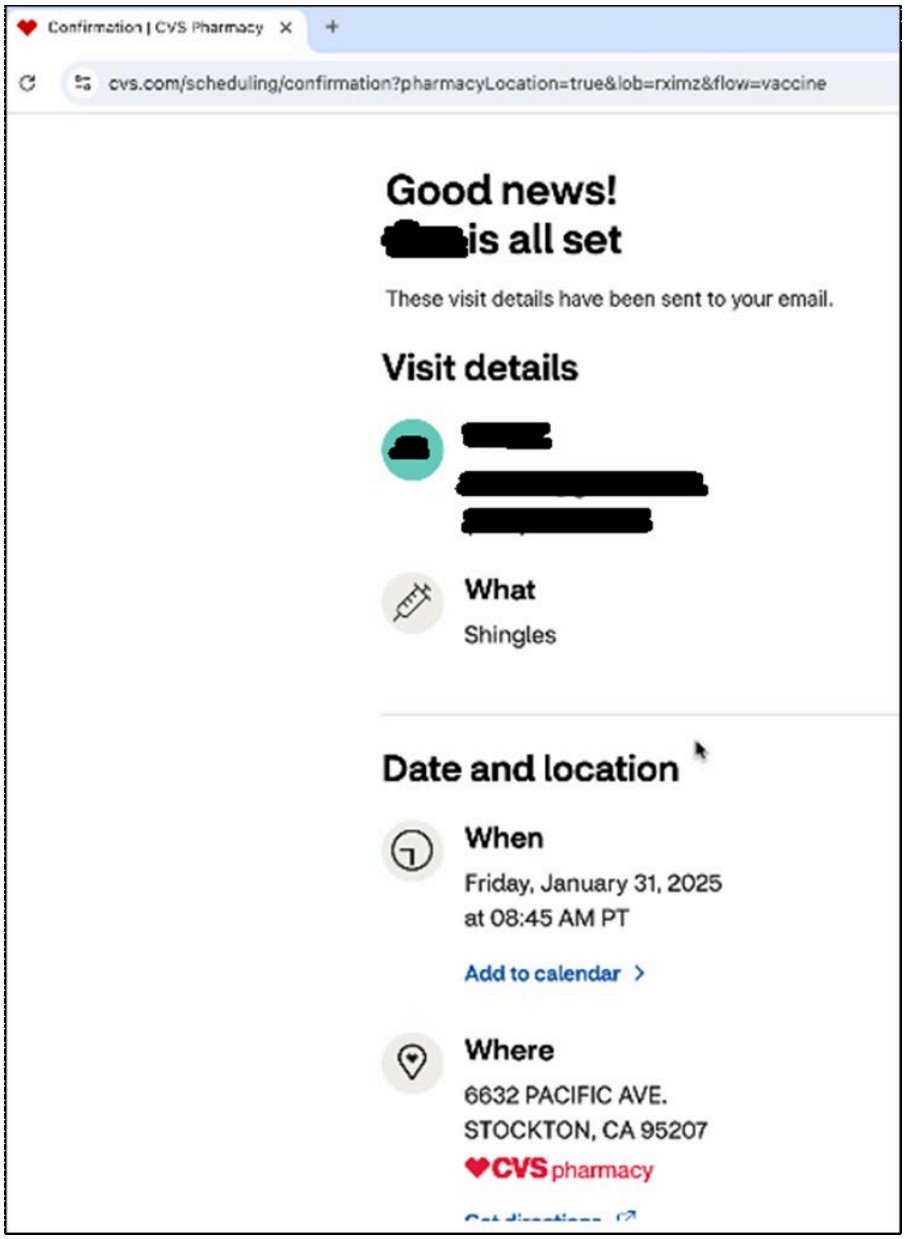


Figure 17C

117. As shown in the redacted website traffic in Figure 18, below, that corresponds with the web images displayed in Figure 17A-C, the Adobe Trackers, as created by Adobe and implemented by CVS, intercept Website users' Private Information, including the name of the vaccine that the Website user confirmed an appointment to receive. Highlighted in yellow, the Adobe Trackers transmitted to Adobe the exact name of the vaccine—in this case, "shingles"—

and the location of the appointment, in this case, store ID "9830," the street address of which is readily available online.[52] Regardless of the type of vaccine selected, the Adobe Tracker is programmed to systematically intercept the type of vaccine for which Website users reserved appointments to have administered. Additionally, highlighted in purple, the Adobe Tracker also assigns and tracks unique identifiers assigned to Website users and their activity on the Website, which are used, as described above, to individually identify them.

118. The web image and code depicted in Figures 17A-C and 18 (below) reflect the activities of Website users that are proceeding as guests. However, the Adobe Trackers intercept the same substantive information reflected in these figures when a Website user is logged in, except that, when logged in, Adobe also intercepts additional persistent user identifiers, such as a PPID, which CVS transmits to allow Adobe to recognize logged in users and associate the user's behavior across visits.

POST https://edge.adobedc.net/ee/or2/v1/interact?configId=314340a7-24fa-4366-890e-088383dc0cd9&requestId=[redacted]4 HTTP/2 content-length: 2741 cache-control: max-age=0 sec-ch-ua-platform: "macOS" user-agent: Mozilla/5.0 [redacted]sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132" content-type: text/plain; charset=UTF-8 sec-ch-ua-mobile: ?0 accept: */* origin: https://www.cvs.com sec-fetch-site: cross-site sec-fetch-mode: cors sec-fetch-dest: empty referer: https://www.cvs.com/scheduling/confirmation?pharmacyLocation=true&lob=rximz&flow=vaccine accept-encoding: gzip, deflate, br, zstd accept-language: en-US,en;q=0.9 priority: u=1, i host: edge.adobedc.net
{"meta":{"configOverrides":{},"state":{"domain":"cvs.com","cookiesEnabled":true,"entries":[{"key":"kndctr [redacted] AdobeOrg_cluster","value":"or2"},{"key":"kndctr [redacted] AdobeOrg_identity","value":"CiY [redacted]="}]}},"events":[{"xdm":{"web":{"webPageDetails":{"URL":"https://www.cvs.com/scheduling/confirmation?pharmacyLocation=true&lob=rximz&flow=vaccine","pageViews":{"value":1},"siteSection":"usf","viewName":"cvs|dweb|scheduling|confirmation|usf:scheduling:confirmation"},"webReferrer":{"URL":"https://www.cvs.com/?icid=cvsheader:cvslogo"}},"device":{"screenHeight":982,"screenWidth":1512,"screenOrientation":"landscape"},"environment":{"type":"browser","browserDetails":{"viewportWidth":1512,"viewportHeight":857}},"placeContext":{"localTimezoneOffset":-

[52] CVS, https://www.cvs.com/store-locator/stockton-ca-pharmacies/6632-pacific-ave-stockton-ca-95207/storeid=9830.

60,"localTime":"[redacted]"},"timestamp":"[redacted]","implementationDetails":{"name":"https://ns.adobe.com/experience/alloy","version":"2.19.2","environment":"browser"},"eventType":"web.webPageDetails.pageViews","_experience":{"analytics":{"customDimensions":{"eVars":{"eVar4":"cvs|dweb|scheduling|confirmation|usf:scheduling:confirmation","eVar49":"www.cvs.com/scheduling/confirmation","eVar41":"dweb","eVar26":"tweb","eVar38":"www.cvs.com","eVar35":"false","eVar3":"usf:digital","eVar57":"usf","eVar11":"rx","eVar12":"patient_number:1_of_1","eVar31":"rx registration status unknown","eVar32":"vax_upsell:denied","eVar51":"Review Visit | CVS Pharmacy","eVar52":"pharmacyLocation=true&lob=rximz&flow=vaccine","eVar55":"filter_not_applied","eVar78":"rx: immunizations: store_rx","eVar89":"9830","eVar106":"CA","eVar109":"list_view:1:locator_results","eVar111":"8-9","eVar138":"Shingles","eVar46":"p1:1_Shingles","eVar37":"p1:1_SHI","eVar159":"lob:rximz","eVar160":"rx_imz","eVar129":"self","eVar182":1,"eVar142":"tphrm=|mcvc2=on|ngs=|ga=g2|rbh2=off|mcpr=|hdau=|mcpe=bl|rxp=on|uh=|mvpe=gr|hp_uh=|canary=|ebe=|mca1=on","eVar143":"on","eVar25":"mfa_not found","eVar102":"login from imz flow:n","eVar152":"mobile_and_email","eVar9":"rx imz: individual","evar22":"22b97a85c60588115de847f9e9520965","eVar84":"covid_vax_preference:on"},"props":{"prop23":"www.cvs.com/scheduling/confirmation","prop11":"dweb","prop47":"1/31/2025 9:28 AM","prop75":"web view|mc profile","prop3":"usf:scheduling:confirmation","prop5":"usf","prop15":"same day","prop48":"prod","prop52":"pharmacyLocation=true&lob=rximz&flow=vaccine","prop43":"self","prop9":"rx: 9830"},"hierarchies":{"hier1":{"values":["cvs|dweb|scheduling|confirmation"]}}}}}},"data":{"__adobe":{"analytics":{"list2":"ld--dhs-ngs-legacy-confirmation"}}}},"query":{"identity":{"fetch":["ECID"]}}}

Figure 18

119. Additionally, while discovery is required to confirm the full extent of Private Information exchanged between Adobe and Criteo, upon information and belief, Adobe shares information it intercepts with Criteo, including but not limited to this page view information and URLS, and unique identifiers, permitting Criteo to further enhance its own customer profiles by synchronizing and cross referencing Criteo's data with information Adobe collects and stores in its ad ecosystem.

4. Scheduling MinuteClinic Appointments

120. The Website also invites Website users to communicate their symptoms or required medical procedures and confirm a virtual or in-person MinuteClinic appointment with a provider to receive medical treatment. CVS advertises its MinuteClinic as providing "high-quality health care[…] For everyone" and allowing Website users to choose from 195 services offered by CVS'

providers.[53] CVS promises that its "providers must be board certified and go through a continuous education process," and ensures that "you get the same great medical care at any of our locations across the country."[54] As depicted below in Figures 19A, 19B, and 19C, as redacted, after entering information describing Website users' symptoms or required procedure, the Website requires users to confirm the details of their submission, including their name, email address, phone number, symptoms for which they are seeking treatment or requested medical procedure, and the date, time, and location of the appointment.[55] CVS requires Website users to confirm information they submitted to confirm their appointments.

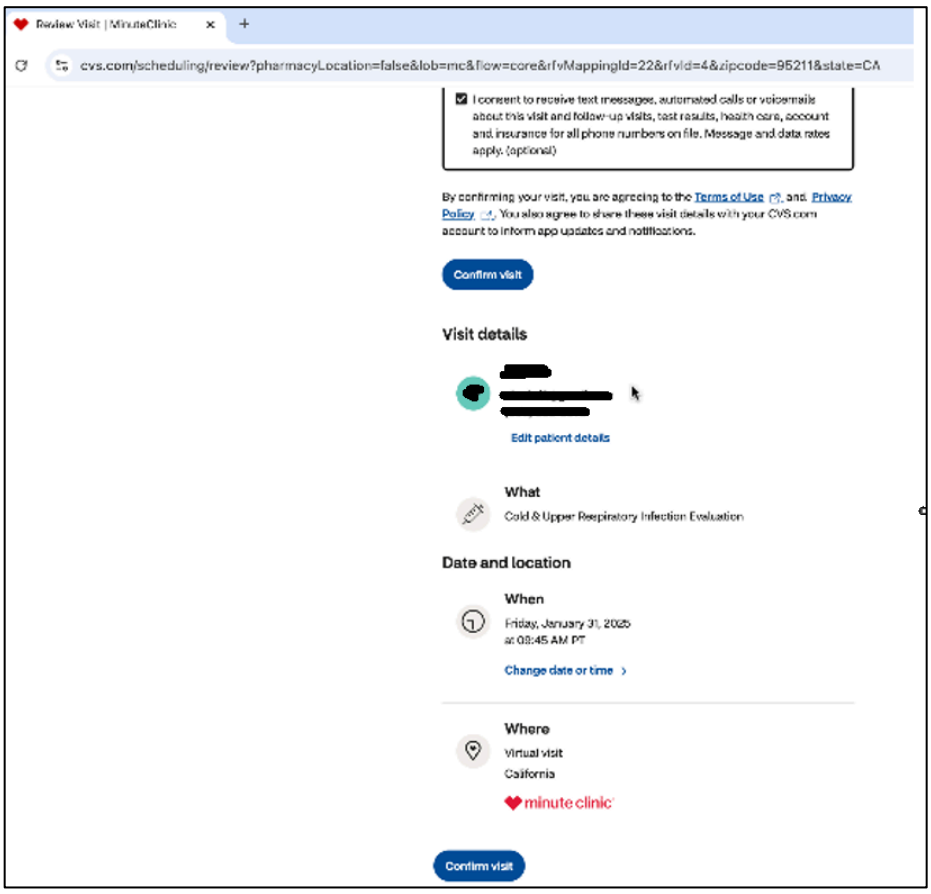


Figure 19A

[53] https://www.cvs.com/minuteclinic
[54] *Id.*
[55] *See* https://www.cvs.com/minuteclinic

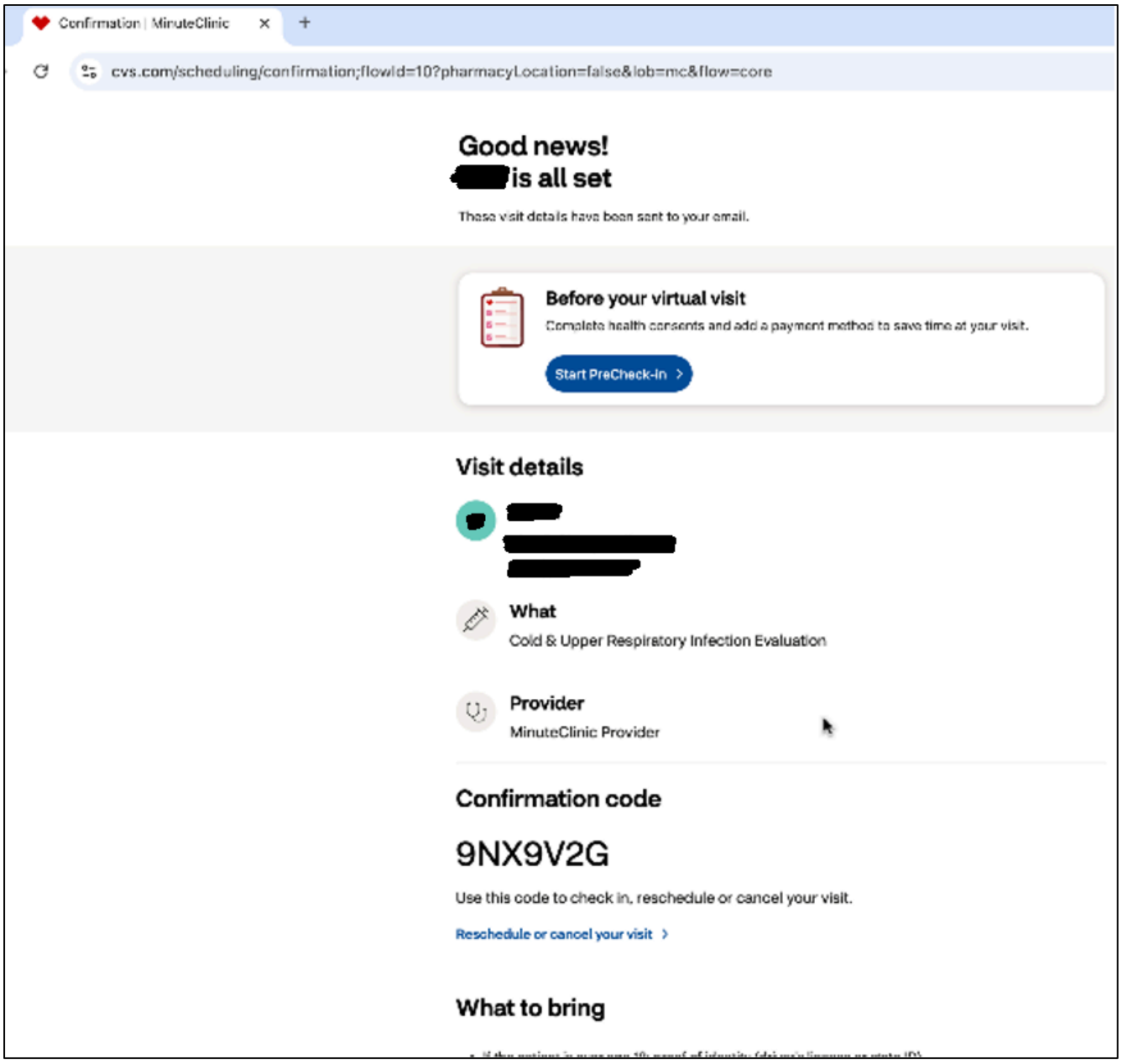

Confirmation | MinuteClinic
cvs.com/scheduling/confirmation;flowId=10?pharmacyLocation=false&lob=mc&flow=core
Good news!
[redacted] is all set
These visit details have been sent to your email.
Before your virtual visit
Complete health consents and add a payment method to save time at your visit.
Start PreCheck-in
Visit details
[redacted]
What
Cold & Upper Respiratory Infection Evaluation
Provider
MinuteClinic Provider
Confirmation code
9NX9V2G
Use this code to check in, reschedule or cancel your visit.
Reschedule or cancel your visit
What to bring

Figure 19B

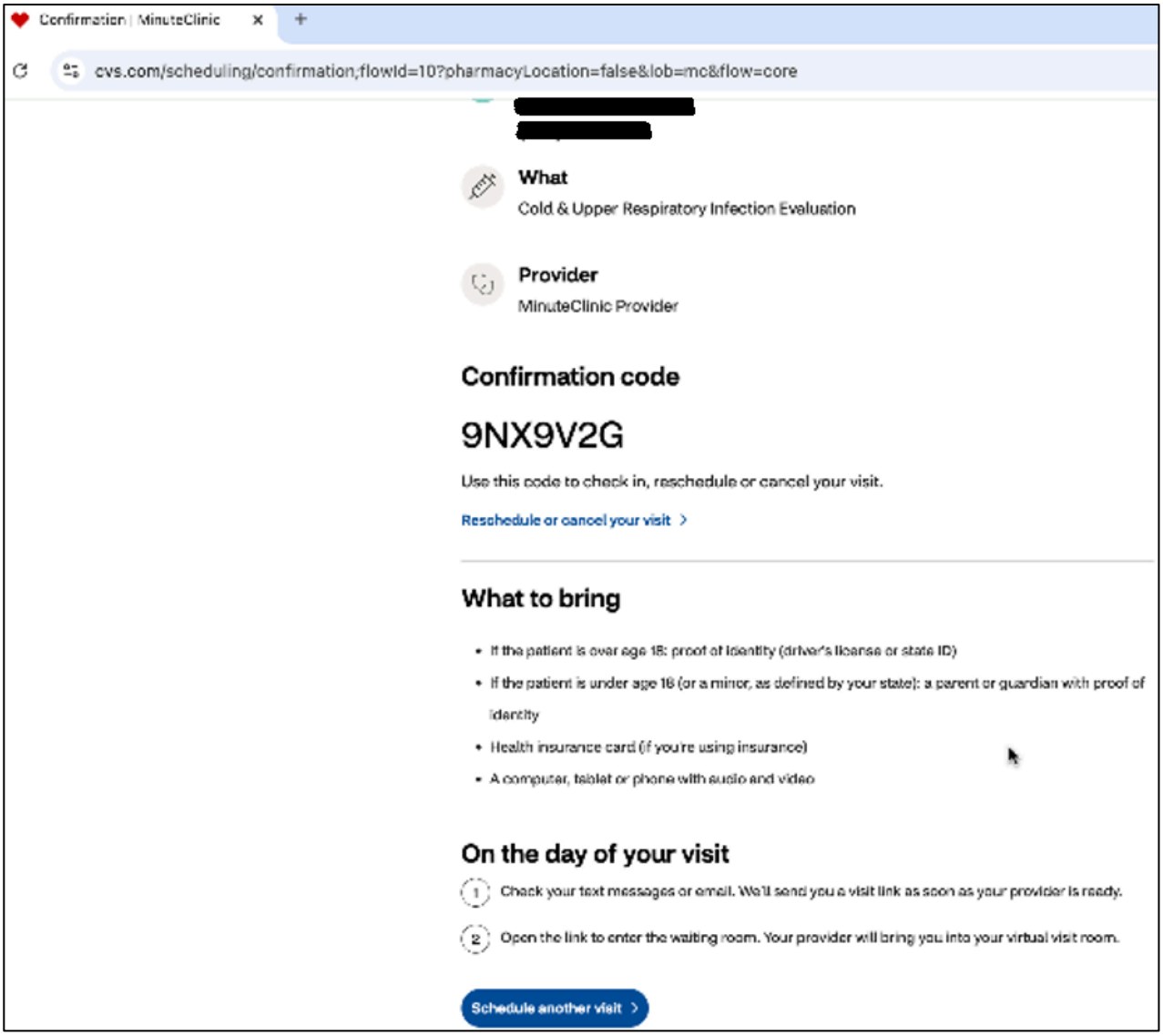


Figure 19C

121. As shown in the redacted website traffic in Figure 20, below, that corresponds with the web images displayed in Figures 19A-19C, the Adobe Trackers, as implemented by CVS, intercept Website users' Private Information, including a description of the symptoms for which treatment is required or description of the requested medical procedures. Highlighted in yellow, the Adobe Trackers transmitted to Adobe this description as entered by the Website user—in this case, "Illness, Infection, or Injury" and "Cold & Upper Respiratory Infection Evaluation." Regardless of the type of symptoms or requested procedures that Website users enter, the Adobe

Tracker is programmed to systematically intercept the symptoms or requested procedures. Additionally, highlighted in purple, the Adobe Tracker also assigns and tracks unique identifiers assigned to Website users' activity on the Website, which are used, as described above, to individually identify the Website user.

122. The web images and traffic depicted in Figures 19 and 20 reflect the activities of Website users proceeding as guests. However, the Adobe Trackers intercept the same substantive information reflected in these figures when a Website user is logged in, except that, when logged in, Adobe also intercepts additional persistent user identifiers, such as a PPID, which CVS transmits to allow Adobe to recognize logged in users and associate the user's behavior across visits.

POST https://edge.adobedc.net/ee/or2/v1/interact?configId=314340a7-24fa-4366-890e-088383dc0cd9&requestId=[redacted] HTTP/2 content-length: 3046 cache-control: max-age=0 sec-ch-ua-platform: "macOS" user-agent: Mozilla/5.0 [redacted] sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132" content-type: text/plain; charset=UTF-8 sec-ch-ua-mobile: ?0 accept: */* origin: https://www.cvs.com sec-fetch-site: cross-site sec-fetch-mode: cors sec-fetch-dest: empty referer: https://www.cvs.com/scheduling/confirmation;flowId=10?pharmacyLocation=false&lob=mc&flow=core accept-encoding: gzip, deflate, br, zstd accept-language: en-US,en;q=0.9 priority: u=1, i host: edge.adobedc.net
{"meta":{"configOverrides":{},"state":{"domain":"cvs.com","cookiesEnabled":true,"entries":[{"key":"kndctr [redacted] AdobeOrg_cluster","value":"or2"},{"key":"kndctr [redacted] AdobeOrg_identity","value":"CiY1MzcxMzY4[redacted]="}]}},"events":[{"xdm":{"web":{"webPageDetails":{"URL":"https://www.cvs.com/scheduling/confirmation;flowId=10?pharmacyLocation=false&lob=mc&flow=core","pageViews":{"value":1},"siteSection":"usf","viewName":"cvs|dweb|scheduling|confirmation;flowid=10|usf:scheduling:confirmation"},"webReferrer":{"URL":"https://www.cvs.com/minuteclinic?icid=cvs-home-s1-l3-health-visit-trgtperf"}},"device":{"screenHeight":982,"screenWidth":1512,"screenOrientation":"landscape"},"environment":{"type":"browser","browserDetails":{"viewportWidth":2016,"viewportHeight":1143}},"placeContext":{"localTimezoneOffset":-60,"localTime":"[redacted]"},"timestamp":"[redacted]","implementationDetails":{"name":"https://ns.adobe.com/experience/alloy","version":"2.19.2","environment":"browser"},"eventType":"web.webPageDetails.pageViews","_experience":{"analytics":{"customDimensions":{"eVars":{"eVar4":"cvs|dweb|scheduling|confirmation;flowid=10|usf:scheduling:confirmation","eVar49":"www.cvs.com/scheduling/confirmation;flowId=10","eVar41":"dweb","eVar26":"dweb","eVar38":"www.cvs.com","eVar3

5":"false","eVar3":"usf:digital","eVar57":"usf","eVar11":"virtual","eVar12":"clinic_selected:no_badge","eVar31":"rx registration status unknown","eVar32":"vax_upsell:denied","eVar51":"Review Visit | MinuteClinic","eVar52":"pharmacyLocation=false&lob=mc&flow=core","eVar55":"filter_not_applied","eVar78":"mc:core:schedule","eVar89":"virtual","eVar106":"CA","eVar108":"visit_type:virtual","eVar109":"list_view:1:locator_results","eVar110":"usf:location:not_preselected","eVar86":"mfa:y|mrn_id:n|rx_connect_id:n","eVar111":"9-10","eVar138":"c1:Illness, Infection, or Injury","eVar37":"s1:Cold & Upper Respiratory Infection Evaluation","eVar159":"lob:mc","eVar160":"mc:other","eVar129":"self","eVar142":"tphrm=|mcvc2=on|ngs=on|ga=g2|rbh2=off|mcpr=|hdau=|mcpe=bl|rxp=on|uh=|mvpe=gr|hp_uh=|canary=|ebe=|mca1=on","eVar143":"on","eVar25":"mfa_not found","eVar102":"login from mc flow:n","eVar119":"pcp:disabled","eVar151":"ngs:mc_core","evar22":"22b97a85c60588115de847f9e9520965","eVar74":"virtual_visit:eligible","eVar157":"provider_type:generic"},"props":{"prop23":"www.cvs.com/scheduling/confirmation;flowId=10","prop11":"dweb","prop47":"1/31/2025 9:48 AM","prop13":"usf:duplicate:false","prop75":"web view|mc profile","prop3":"usf:scheduling:confirmation","prop5":"usf","prop15":"same day","prop48":"prod","prop52":"pharmacyLocation=false&lob=mc&flow=core","prop43":"self","prop14":"consent_to_contact:n","prop9":"virtual"},"hierarchies":{"hier1":{"values":["cvs|dweb|scheduling|confirmation;flowId=10"]}}}}}},"data":{"__adobe":{"analytics":{"list2":"ld--dhs-ngs-legacy-confirmation"}}}},"query":{"identity":{"fetch":["ECID"]}}}

Figure 20

5. Managing Prescription Drugs

123. The Website also invites Website users with accounts to log in and manage and refill their prescription drugs.[56] As depicted below in Figure 21, as redacted, CVS requires Website users to confirm information they submitted to fill prescriptions, including their name, the name, phone number, and fax number of the prescriber, and details of the prescription to be filled, including the drug name: in this case—Amoxicillin 500 Mg Capsule.

//

//

//

//

//

//

[56] *See* https://www.cvs.com/pharmacy

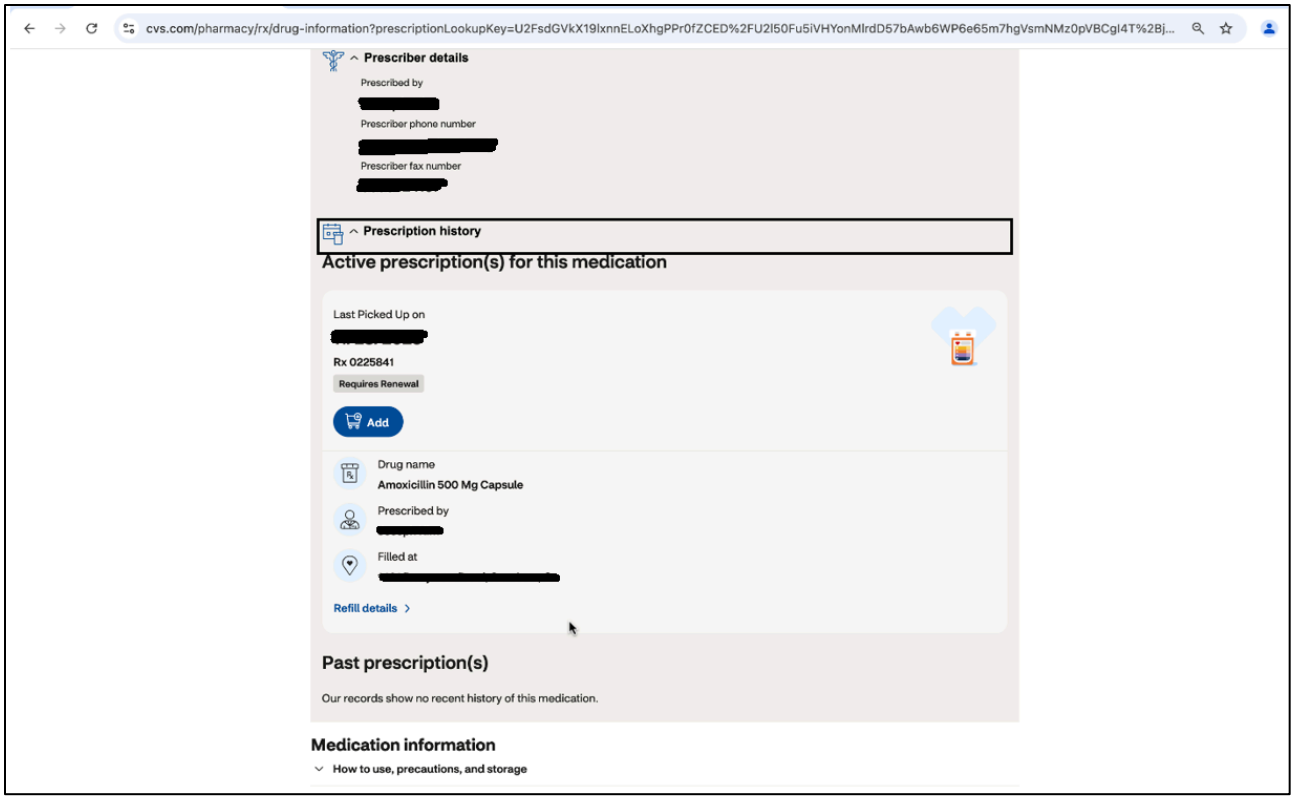


Figure 21

124. As shown in the redacted website traffic in Figure 22, below, that corresponds with the web image displayed in Figure 21, the Adobe Trackers, as created by Adobe and implemented by CVS, intercept Website users' Private Information, including the name of the prescription drug that the Website user is filling. Highlighted in yellow, the Adobe Trackers transmitted to Adobe this description of the drug's name—"name":"Amoxicillin 500 Mg Capsule". Regardless of the type of prescription to be filled, the Adobe Tracker is programmed to systematically intercept the details of that prescription. Additionally, highlighted in purple, the Adobe Tracker also assigns and tracks unique identifiers assigned to Website users' activity on the Website, which are used, as described above, to individually identify the Website user.

POST https://edge.adobedc.net/ee/or2/v1/collect?configId=c370c17c-eda0-4cf9-bbd9-bcc730cd6d19&requestId=[redacted]6 HTTP/2 host: edge.adobedc.net content-length: 1848 sec-ch-ua-platform: "macOS" user-agent: Mozilla/5.0 [redacted] sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132" content-type: text/plain; charset=utf-8 sec-

ch-ua-mobile: ?0 accept: / origin: https://www.cvs.com sec-fetch-site: cross-site sec-fetch-mode: no-cors sec-fetch-dest: empty referer: https://www.cvs.com/ accept-encoding: gzip, deflate, br, zstd accept-language: en-US,en;q=0.9 priority: u=4, i
{"meta":{"configOverrides":{},"state":{"domain":"cvs.com","cookiesEnabled":true,"entries":[{"key":"kndctr_06660D1556E030D17F000101_AdobeOrg_cluster","value":"or2"},{"key":"kndctr [redacted] AdobeOrg_identity","value":"CiYxNTAyMj[redacted]"}]}},"events":[{"xdm":{"eventType":"web.webinteraction.linkClicks","web":{"webInteraction":{"name":"Amoxicillin 500 Mg Capsule","region":"rx-tile-0","type":"other","URL":"https://www.cvs.com/pharmacy/rx/drug-information?prescriptionId=[redacted]","linkClicks":{"value":1}},"webPageDetails":{"URL":"https://www.cvs.com/pharmacy/rx/prescriptions"},"webReferrer":{"URL":"https://www.cvs.com/?icid=cvsheader:cvslogo"}},"device":{"[redacted]"},"environment":{"type":"browser","browserDetails":{"viewportWidth":1890,"viewportHeight":1071}},"placeContext":{"localTimezoneOffset":-60,"localTime":"[redacted]"},"timestamp":"[redacted]","implementationDetails":{"name":"https://ns.adobe.com/experience/alloy","version":"2.19.2","environment":"browser"},"_experience":{"analytics":{"customDimensions":{"eVars":{"eVar35":"true"}}}}}],"query":{"identity":{"fetch":["ECID"]}}}

Figure 22

125. At all relevant times, with respect to each of the above-described activities taken on the Website, CVS disclosed through the Adobe Trackers Website users' activities on the Website, and aided Adobe's collection, use, and disclosure of it to third parties unbeknownst to Plaintiffs and Class Members. The unique identifiers identified above and in the corresponding web traffic that CVS sent to Adobe allowed Adobe to link the Private Information to specific Website users and identify them.

E. CVS ENABLED CRITEO'S WIRETAPPING OF PLAINTIFFS' ELECTRONIC COMMUNICATIONS VIA THE WEBSITE.

126. In exchange for payment, Criteo offers data collection and advertising services to its customers, including CVS. For instance, upon information and belief, as part of its customer

relationship with CVS, Criteo offered snippets of code to CVS and other tracking services ("Criteo Trackers"), which were designed to track users' activity on the Website, unbeknownst to those users, together with unique identifiers capable of identifying them, for Criteo's and other third-parties' marketing uses. Upon information and belief, the various unique identifiers and information that Criteo intercepts allow it to identify Website users across different devices, visits, and touchpoints, creating a unique customer profile similar to Adobe's Identity Graph.

127. Companies like CVS can (and on information and belief, CVS does) utilize Criteo's advertising platform and services to target specific users. For example, Criteo offers "Lookalike Audiences" that permit its customers to target new customers whose browsing and purchasing behaviors resemble its existing users.

128. Upon information and belief, CVS contracted with Criteo for the implementation of the Criteo Trackers on its Website, after which CVS and Criteo implemented those tracking technologies onto the Website. As a result, CVS disclosed and Criteo intercepted Website users' private communications made to CVS on the Website. Plaintiff and other Website users provided their PII, health information, and other sensitive data to CVS to obtain medical treatment and prescriptions and schedule vaccination and physician appointments without any knowledge these communications would be intercepted by a third-party for its own commercial benefit. In this way, Criteo directly intercepted, at a minimum, Website users' Private Information, including keyword searches and page views, including checkout pages

129. Plaintiffs did not consent—or even know of—Criteo's interception and use of his communications with CVS. Criteo's interception of Plaintiffs' PII, health data, and other highly sensitive information without their consent is an invasion of his privacy and violation of several laws, including the Federal Wiretap Act, 18 U.S.C. § 2511 (also known as the Electronic

Communications Privacy Act, or "ECPA"), HIPAA, the Florida Stored Communications Act, Fla. Stat. § 934.03 *et seq.* ("FSCA"), the California Invasion of Privacy Act, Cal. Penal Code §§ 630 *et seq.* ("CIPA"), and the Maryland Wiretap Act Md. Cts. & Jud. Pro. § 10-401 *et seq.*

130. Specifically, a live data-traffic analysis of CVS' Website showed that Criteo's tracking technologies installed on CVS' Website track these communications, regardless of whether these visitors were signed into the Website or using the Website as a guest. For example, if a Website visitor were to type specific queries into the search bar that appears at the top of CVS' Website, such as "pregnancy test," Criteo would intercept that information in the form of a URL request (as shown below) in yellow highlight. Further, among other identifying information, Criteo assigns numerous unique user identification values to each Website user, used to specifically identify each such visitor, as highlighted in part in blue below. Although not contained in the below traffic, the Criteo Trackers also obtain users' IP addresses.

[redacted]GET https://sslwidget.criteo.com/event?a=57162&v=5.37.0&otl=1&p0=e%3Dvl%26p%3D%255B743786%252C871694%252C298381%252C289586%252C177757%252C378503%252C555693%252C559408%252C430757%252C546712%252C340385%252C184046%252C549555%252C616827%252C398422%252C455366%252C921384%252C192485%252C630020%252C312813%255D%26kw%3Dpregnancy%2520test%26ca%3D%26pnb%3D1%26f%3D%255B%255D&p1=e%3Dexd%26rvi%3D&p2=e%3Ddis&bundle=TszKnV9yaVdTJTJCNVROZGlwUzZud2NWR3ZQb3R4VnhiSTJJY3p4ayUyQmZmbFJqQXBzR2lacUd2M29JMFhMMm91NkFRUndpR1hYZVZoVEtlajFsZTJ2YXZscUFsZ0dScTdrRnJQTTNrNXlKaUFHUnVZZHEwZ1ZTcDY2ZGNmM05iJTJCZ2R3MUpqRVJZTzV1JTJGQnFRRXRlM0klMkZydVRMYXRWclI2eXlCekR3c1dmV0lieG14diUyQlNvVzZvOVZsbFh1VVZ5c0ttUnBjOXM&sc=%7B%22fbp%22%3A%22fb.1.[redacted]&tld=cvs.com&dy=1&fu=https%253A%252F%252Fwww.cvs.com%252Fsearch%253FsearchTerm%253Dpregnancy%252520test&pu=https%253A%252F%252Fwww.cvs.com%252Faccount%252Fcompliance%252Fdo-not-sell&ceid=9a668a3c-8768-40c2-a3e8-e9b2179ae847&consent_cookie=OptanonConsent HTTP/2 sec-ch-ua-platform: "macOS" user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36 sec-ch-ua: "Google Chrome";v="135", "Not-A.Brand";v="8", "Chromium";v="135" sec-ch-ua-mobile: ?0 accept: / sec-fetch-site: cross-site sec-fetch-mode: no-cors sec-fetch-dest: script sec-fetch-storage-access: active referer: https://www.cvs.com/ accept-encoding: gzip, deflate, br, zstd accept-language: en-US,en;q=0.9 cookie: uid=[redacted]; cto_bundle=E[redacted]

134. [redacted]s host: sslwidget.criteo.com

Figure 23

135. Similarly, when Website visitors visit a specific webpage, Criteo intercepts the title of the webpage, including checkout pages, revealing page information in the form of a URL request (as shown below). The website URL is highlighted in yellow below, together with coded information that the product has been added to the user's shopping cart, and one of the unique identifiers Criteo uses to uniquely identify users is highlighted in blue below. In this example, a Website user viewed Aspirin Regiment Baer 81mg Enteric Coasted Tablets for pain relief and added the product to their cart.

GET
https://sslwidget.criteo.com/event?a=%5B57162%5D&v=5.31.1&otl=1&p0=e%3Dvpg&bundle=qJ3rxF9OQiUyRjR2U1JmQnc4YnU1QURKMnVnRUpMVXdCN0VHSXBHNzZXVXByTWNEY0VxSUZ6SU05RjVrMTgxVW5iOWFNYWNMdzdSdlhZTXRlUzBSeGJqS25nZWZZMHg1bDZIdGRtWnoxcyUyRkJ0a2Y4SG1PT0lKdGhwandrUnVLYVl0VnJGcGVLZEZIdEs2b21adW4xSSUyRmFkVDlURnclM0QlM0Q&sc=%7B%22fbp%22%3A%22fb.1.[redacted].[redacted]%22%7D&tld=cvs.com&dy=1&fu=https%253A%252F%252Fwww.cvs.com%252Frx%252Fdotm%252Fcart%253FflowType%253DFS&pu=https%253A%252F%252Fwww.cvs.com%252Fshop%252Faspirin-regimen-bayer-81mg-enteric-coated-tablets-pain-reliever-fever-reducer-300-ct-prodid-1012066&ceid=cfadb42f-b89c-4b0d-96bd-4eb362f840e1 HTTP/2
sec-ch-ua-platform: "macOS"
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
sec-ch-ua-mobile: ?0
accept: */*
sec-fetch-site: cross-site
sec-fetch-mode: no-cors
sec-fetch-dest: script
referer: https://www.cvs.com/
accept-encoding: gzip, deflate, br, zstd
accept-language: en-US,en;q=0.9
cookie: uid=[redacted];
cto_bundle=SwEk1l[redacted]VOE8
host: sslwidget.criteo.com

Figure 24

136. The web images and traffic depicted in Figures 23 and 24 reflect the activities of

Website users proceeding as guests. However, the Adobe Trackers intercept the same substantive information reflected in these figures when a Website user is logged in, except that, when logged in, Adobe also intercepts additional persistent user identifiers, such as a PPID, which CVS transmits to allow Adobe to recognize logged in users and associate the user's behavior across visits.

F. CVS ENABLED MEDALLIA'S WIRETAPPING OF PLAINTIFFS' ELECTRONIC COMMUNICATIONS VIA THE WEBSITE.

137. In exchange for payment, Medallia offers data collection and processing services to its customers including, on information and belief, CVS. As part of its customer relationship with CVS, Medallia offered snippets of code to CVS and other tracking services, which were designed to track users' activity on the Website, unbeknownst to those users, together with unique identifiers capable of identifying them. Medallia's collection of Website users' private information was necessary to target CVS' specific users. Upon information and belief, the various unique identifiers and information that Medallia intercepts allow it to identify Website users across different devices, visits, and touchpoints, creating a unique customer profile similar to Adobe's Identity Graph.

138. Upon information and belief, CVS contracted with Medallia for the implementation of the Medallia Trackers on its Website, after which CVS and Medallia implemented those tracking technologies onto the Website. As a result, CVS disclosed and Medallia intercepted Website users' private communications made to CVS on the Website. Plaintiffs and other Website users provided their PII, health information, and other sensitive data to CVS to obtain medical treatment and prescriptions without any knowledge these communications would be intercepted by a third-party for its own commercial benefit. In this way, Medallia directly intercepted, at a minimum, Website users' Private Information, including keyword searches, prescription medicine,

and page views, including checkout pages.

139. Plaintiffs did not consent to—or even know of—Medallia's interception and use of their communications with CVS. Medallia's interception of Plaintiffs' PII, health data, and other highly sensitive information without their consent is an invasion of their privacy and violation of several laws, including the ECPA, HIPAA, FSCA, CIPA, and the Maryland Wiretap Act.

140. Specifically, a live data-traffic analysis of CVS' Website showed that Medallia's tracking technologies installed on CVS' Website track these communications, regardless of whether these visitors were signed into the Website or using the Website as a guest. For example, if a Website visitor was to type specific queries into the search bar that appears at the top of CVS' Website, such as "pregnancy test," Medallia would intercept that information in the form of a URL request (as shown below) in yellow highlight. Further, among other identifying information, Medallia assigns numerous unique user identification values to each Website user, used to specifically identify each such visitor, as highlighted in part in blue below.

POST https://analytics-fe.digital-cloud.medallia.com/api/web/events HTTP/2 content-length: 1676 mec-integration-id: cvs-sc4-medallia-com-cvs sec-ch-ua-platform: "macOS" user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36 sec-ch-ua: "Google Chrome";v="135", "Not-A.Brand";v="8", "Chromium";v="135" content-type: application/json charset: UTF-8 sec-ch-ua-mobile: ?0 accept: / origin: https://www.cvs.com sec-fetch-site: cross-site sec-fetch-mode: cors sec-fetch-dest: empty referer: https://www.cvs.com/ accept-encoding: gzip, deflate, br, zstd accept-language: en-US,en;q=0.9 priority: u=1, i host: analytics-fe.digital-cloud.medallia.com
[{"sessionScreenSize":"1512x982","sessionDua":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36","sessionPlatform":"MacIntel","referringUrl":"https://www.cvs.com/account/compliance/do-not-sell","pageTitle":"Shop Beauty, Vitamins, Medicine & Everyday Essentials | CVS.com","pageUrl":"https://www.cvs.com/search?searchTerm=pregnancy%20test","type":"website","eventName":"nebula_after_http_get_request","timestamp":"[redacted]","eventTimezoneOffset":2,"accountId":[redacted],"propertyId":[redacted],"formId":null,"formTriggerType":null,"mdData":{"submittedDate":"","declinedDate":"1745925355656","lastInvitationView":"1745925351748","mdUserPercentile":"13.831256956179027","mdInvitePresented":"true","httpRequestData":{"requestUrl":"https://resources.digital-cloud.medallia.com/wdcus/183558/forms/12868/invitationData1706638460824_en.json","attemptNumber":0,"requestTotalTimeInSeconds":0.007}},"userId":"[redacted]","sessionId":"[redacted]","cookieSize":10561,"sdkVersion":"2.58.1","historyLengt

h":4,"isUserIdentified":false,"clientHints":"{\"architecture\":\"arm\",\"bitness\":\"64\",\"brands\":[{\"brand\":\"Google Chrome","version":"135"},{"brand":"Not-A.Brand","version":"8"},{"brand":"Chromium","version":"135"}],"fullVersionList":[{"brand":"Google Chrome","version":"135.0.7049.115"},{"brand":"Not-A.Brand","version":"8.0.0.0"},{"brand":"Chromium","version":"135.0.7049.115"}],"mobile":false,"model":"","platform":"macOS","platformVersion":"15.4.1","uaFullVersion":"135.0.7049.115","wow64":false}"}]

Figure 27

141. Similarly, when Website visitors visit a specific webpage, Medallia intercepts the title of the webpage, including checkout pages, revealing page information in the form of a URL request (as shown below). The website URL is highlighted in yellow below, and several of the identifiers Medallia uses to uniquely identify users are highlighted in blue below. In this example, a Website user viewed a three-pack of Clearblue Early Digital Pregnancy Tests.

POST https://analytics-fe.digital-cloud.medallia.com/api/web/events HTTP/2 content-length: 1798 mec-integration-id: cvs-sc4-medallia-com-cvs sec-ch-ua-platform: "macOS" user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36 sec-ch-ua: "Google Chrome";v="135", "Not-A.Brand";v="8", "Chromium";v="135" content-type: application/json charset: UTF-8 sec-ch-ua-mobile: ?0 accept: / origin: https://www.cvs.com sec-fetch-site: cross-site sec-fetch-mode: cors sec-fetch-dest: empty referer: https://www.cvs.com/ accept-encoding: gzip, deflate, br, zstd accept-language: en-US,en;q=0.9 priority: u=1, i host: analytics-fe.digital-cloud.medallia.com
[{"sessionScreenSize":"1512x982","sessionDua":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36","sessionPlatform":"MacIntel","referringUrl":"https://www.cvs.com/search?searchTerm=pregnancy%20test","pageTitle":"Clearblue Early Digital Pregnancy Test, Early Detection at Home Pregnancy Test, 3 CT (FSA Eligible) - CVS Pharmacy","pageUrl":"https://www.cvs.com/shop/clearblue-early-digital-pregnancy-test-early-detection-at-home-pregnancy-test-3-ct-prodid-743786","type":"website","eventName":"nebula_after_http_get_request","timestamp":"[redacted]","eventTimezoneOffset":2,"accountId":[redacted],"propertyId":[redacted],"formId":null,"formTriggerType":null,"mdData":{"submittedDate":"","declinedDate":"1745925355656","lastInvitationView":"1745925351748","mdUserPercentile":"13.831256956179027","mdInvitePresented":"true","httpRequestData":{"requestUrl":"https://resources.digital-cloud.medallia.com/wdcus/183558/forms/12868/invitationData1706638460824_en.json","attemptNumber":0,"requestTotalTimeInSeconds":0.032}},"userId":"[redacted]","sessionId":"[redacted]","cookieSize":11166,"sdkVersion":"2.58.1","historyLength":5,"isUserIdentified":false,"clientHints":"{\"architecture\":\"arm\",\"bitness\":\"64\",\"brands\":[{\"brand\":\"Google Chrome","version":"135"},{"brand":"Not-A.Brand","version":"8"},{"brand":"Chromium","version":"135"}],"fullVersionList":[{"brand":"Google Chrome","version":"135.0.7049.115"},{"brand":"Not-A.Brand","version":"8.0.0.0"},{"brand":"Chromium","version":"135.0.7049.115"}],"mobile":false,"model":"","platform":"macOS","platformVersion":"15.4.1","uaFullVersion":"135.0.7049.115","wow64":false}"}]

Figure 28

142. The web images and traffic depicted in Figures 27 and 28 reflect the activities of Website users proceeding as guests. However, the Medallia Trackers intercepts the same substantive information reflected in these figures when a Website user is logged out as they do when a user is logged in.

143. Additionally, as shown in Figure 16, below, when Website users log into the patient portal to manage their prescriptions, the Medalia Trackers, as created by Medallia and implemented by CVS and Medallia, intercept Website users' Private Information, including the name of the prescription drug that the Website user is filling. Highlighted in yellow, the Medallia Trackers transmitted to Medallia this description of the drug's name—"name":"Amoxicillin 500 Mg Capsule". Regardless of the type of prescription to be filled, the Medallia Tracker is programmed to systematically intercept the details of that prescription. Additionally, highlighted in blue, the Medallia Trackers also assigns and tracks unique identifiers assigned to Website users' activity on the Website, which are used to individually identify the Website user.

POST https://analytics-fe.digital-cloud.medallia.com/api/web/events HTTP/2 content-length: 2288 mec-integration-id: cvs-sc4-medallia-com-cvs sec-ch-ua-platform: "Windows" user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36 sec-ch-ua: "Google Chrome";v="135", "Not-A.Brand";v="8", "Chromium";v="135" content-type: application/json charset: UTF-8 sec-ch-ua-mobile: ?0 accept: / origin: https://www.cvs.com sec-fetch-site: cross-site sec-fetch-mode: cors sec-fetch-dest: empty referer: https://www.cvs.com/ accept-encoding: gzip, deflate, br, zstd accept-language: en-US,en;q=0.9 priority: u=1, i host: analytics-fe.digital-cloud.medallia.com
[{"sessionScreenSize":"1600x900","sessionDua":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36","sessionPlatform":"Win32","referringUrl":"https://www.cvs.com/pharmacy/rx/prescriptions","pageTitle":"Amoxicillin 500 Mg Capsule CAP 500 Mg - Amoxil - Dosage, Side Effects & Drug Information - CVS Pharmacy","pageUrl":"https://www.cvs.com/pharmacy/rx/drug-information?prescriptionLookupKey=U2FsdGVkX186%2F8kj5pZT9PLxF%2FnZGZRom4lYHtDE%2F4SRvJbDhYJqoxKd0H8rMJcmeU9pDhX0ObM3hRRvc1qtlt%2BJuAzKzCVP9gI2fflbOE3eOXFSJnqd%2BJsRlHP7TGjB8PaZm9iupASJXXKLMzpOr0w2En3xZ%2FzMwpR1Fh0Fo9W0UipczxI4IySifiorEG7mnKJnDF6YGa0mdxE9KwsxGlP64KPy9xPloDMVEQXt%2Bu3ZpIEAxGk9Wqo%2BJotj%2BcfNN%2F4NxTcOXbdQxLk5JggAJZ1YdrrwrfbYwx4Sfg22N2B5pN2kgbwmDbh4qgnnZx0K%2BzF0cLRwJRf%2F0ZBqAzH%2FQWy0gpErzclV91

RAtuDZqY3vov3NmEWOhWbKn%2BXbGXMOEVhrMI6%2Fz7Q3a6CYD0I2SCrWFRZD
ACFHtyEakgiwn7sfL9RbqBo2Ib0KH7ZdFbCaNMxLtKJGfZAUd69ozC49WK%2FabiWK0o
XQfLyiSdqJK35ja40X2mfJ6xE%2FyKrv68Dsuta8cyZlmq2gxKKbORI81g%3D%3D","type":
"website","eventName":"nebula_after_http_get_request","timestamp":"[redacted]
[redacted]","eventTimezoneOffset":-
7,"accountId":[redacted],"propertyId":[redacted],"formId":null,"formTriggerType":null,"mdData":{
"submittedDate":"","declinedDate":"1746030428256","lastInvitationView":"1746030412502",
"mdUserPercentile":"98.86651731299457","mdInvitePresented":"","httpRequestData":{"requ
estUrl":"https://resources.digital-
cloud.medallia.com/wdcus/183558/forms/9664/formDataV2_1741173789635_en.json","attem
ptNumber":0,"requestTotalTimeInSeconds":0.135}},"userId":"[redacted]
[redacted]","sessionId":"[redacted]","cookieSize":11395,"sdkVersion":"2.58.1","historyLengt
h":15,"isUserIdentified":false,"clientHints":"{\"architecture\":\"x86\",\"bitness\":\"64\",\"brand
s\":[{\"brand\":\"Google Chrome","version":"135"},{"brand":"Not-
A.Brand","version":"8"},{"brand":"Chromium","version":"135"}],"fullVersionList":[{"brand"
:"Google Chrome","version":"135.0.7049.115"},{"brand":"Not-
A.Brand","version":"8.0.0.0"},{"brand":"Chromium","version":"135.0.7049.115"}],"mobile":f
alse,"model":"","platform":"Windows","platformVersion":"19.0.0","uaFullVersion":"135.0.70
49.115","wow64":false}"}]

Figure 29

G. PLAINTIFFS AND CLASS MEMBERS HAVE A REASONBALE EXPECTATION OF PRIVACY OVER THEIR COMMUNICATIONS WITH CVS.

144. Website and Application users had a reasonable expectation of privacy in the Private Information they communicated with CVS via the Website and Application, such as: search terms about health conditions for which they sought health care services and products; their managing of prescription drugs; their contacting of healthcare providers to make appointments for the administration of vaccines and MinuteClinic appointments; and details of the healthcare products, drugs, and vaccines, and symptoms/requested medical procedures about which Website users communicated with CVS on the Website.

145. Defendants' disclosure and/or interception of Plaintiffs' and Class Members' Private Information also violated HIPAA. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care

provider," (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 either (i) "identifies the individual;" or (ii) "[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.

146. HIPAA prohibits health care providers from "us[ing] or disclos[ing] 'protected health information' except as permitted or required by" the HIPAA Privacy Rule. 45 C.F.R. § 1644.502.

147. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be PHI. The Department of Health and Human Services ("HHS") has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phone book because it is not related to health data, "[i]f such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI."[57]

148. The HHS has also issued the following guidance:

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

[57] U.S. Department of Health and Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule; https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (accessed July 9, 2025).

the list.[58]

149. The Office for Civil Rights ("OCR") at HHS previously issued a statement titled "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates" discussing the use of the Meta Pixel by healthcare organizations:

> 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.[59]

150. HHS's view of PHI is broad:

> [Individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.[60]

151. Commenting on a June 2022 report discussing the similar use of the Meta Pixel by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy advisor at HHS, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it . . . It is quite likely a HIPAA

[58] U.S. Department of Health and Human Services, Marketing; https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html (accessed July 9, 2025).
[59] U.S. Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates; https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (accessed July 9, 2025).
[60] *Id*.

violation."[61]

152. As such, Plaintiffs and Class Members had every reason to believe the Private Information they communicated to CVS through the Website would be protected, rather than shared with Adobe, Criteo, Medallia, QM, and other third parties for marketing purposes.

H. PLAINTIFFS' AND CLASS MEMBERS' PRIVATE INFORMATION HAD FINANCIAL VALUE, AND PLAINTIFFS AND CLASS MEMBERS WERE HARMED.

153. As stated in a 2017 feature story in *The Economist*, the "world's most valuable resource is no longer oil, but data."[62] 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.").

154. For example, in 2015, *TechCrunch* reported that "to obtain a list containing the names of individuals suffering from a particular disease," a market participant would have to spend about "$0.30 per name." That same article noted that "[d]ata has become a strategic asset that allows companies to acquire or maintain a competitive edge," and that the value of a single user's data (within the corporate acquisition context) can vary from $15 to more than $40 per user.[63]

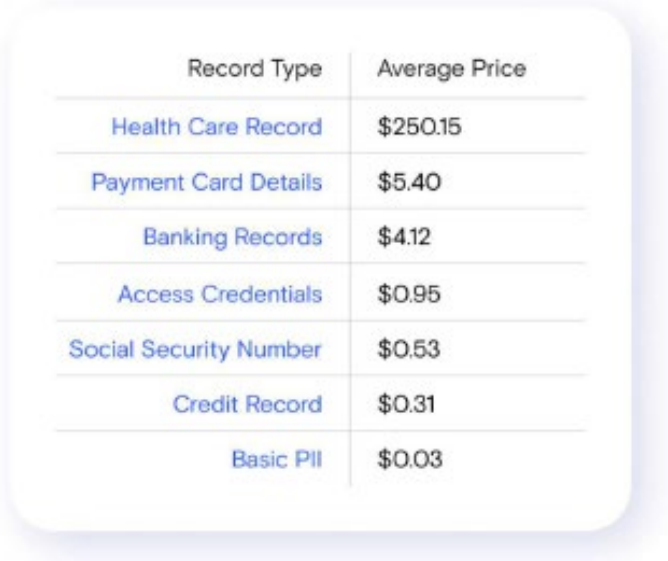
155. A report from *Invisibly* found that protected medical information is one of the most

[61] Advisory Board, 'Deeply troubled': Security experts worry about Facebook trackers on hospital sites; https://www.advisory.com/daily-briefing/2022/06/17/data-trackers (accessed July 9, 2025).
[62] The Economist, The world's most valuable resource is no longer oil, but data; https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (accessed July 9, 2025).
[63] TechCrunch, What's the Value of Your Data?; https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (accessed July 9, 2025).

valuable pieces of data within this data market.

> It's worth acknowledging that because health care records often feature a more complete collection of the patient's identity, background, and PII, health care records have proven to be of particular value for data thieves. While a single social security number might go for $0.53, a complete health care record sells for $250 on average. For criminals, the more complete a dataset, the more potential value they can get out of it. As a result, healthcare breaches increased 55% in 2020.[64]

156. *Invisibly* also noted the following breakdown in average price for record type:



Record Type	Average Price
Health Care Record	$250.15
Payment Card Details	$5.40
Banking Records	$4.12
Access Credentials	$0.95
Social Security Number	$0.53
Credit Record	$0.31
Basic PII	$0.03

Figure 30

157. With regard to health care data specifically, CNBC reported in 2020 that hospital executives were receiving a growing number of bids for user data:

> Hospitals, many of which are increasingly in dire financial straits, are weighing a lucrative new opportunity: selling patient health information to tech companies.
>
> * * *
>
> De-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.

[64] Invisibly, How Much is Your Data Worth? The Complete Breakdown for 2021; https://web.archive.org/web/20250121040219/https://www.invisibly.com/learn-blog/how-much-is-data-worth/ (accessed July 9, 2025).

> Just one company alone, IQVIA, said on its website that it has access to more than 600 million patients records globally that are nonidentified, much of which it accesses through provider organizations. The buyers, which include pharma marketers, will often use it for things like clinical trial recruiting.[65]

158. Likewise, individuals can sell or monetize their own data if they so choose. As an example, Facebook has previously offered to pay individuals for their voice recordings,[66] and has paid teenagers and adults up to $20 a month plus referral fees to install an application that allows Facebook to collect data on how individuals use their smartphones.[67] Numerous other companies and applications such as Nielsen Data, Killi, DataCoup, and AppOptix offer consumers money in exchange for their personal data.[68]

159. CVS provides no such compensation to Plaintiffs and the Class Members in exchange for their surreptitiously obtained Private Information, but they should be held financially accountable to Plaintiffs and Class Members under the laws sought to be enforced in this lawsuit.

CLASS ACTION ALLEGATIONS

160. Plaintiffs seek to represent all persons who have accessed any of CVS' digital or web-based properties, including, but not limited to the CVS Website, CVSHealth.com, and the CVS App in the United States during the relevant statute of limitations period for the claims and through the date of preliminary approval (the "Class").

---

[65] CNBC, Hospital execs say they are getting flooded with requests for your health data; https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (accessed July 9, 2025).

[66] The Verge, Facebook Will Now Pay You for Your Voice Recordings; https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognitionviewpoints-prounciations-app (accessed July 9, 2025).

[67] CNBC, *Facebook Pays Teens to Install An App That Could Collect All Kinds of Data*; https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html (accessed July 9, 2025).

[68] DOLLAR BREAK, 10 Best Data Collection Apps (Get Paid to Share Your Data)*: Earn a Passive Income*; https://www.dollarbreak.com/apps-that-pay-you-for-data-collection/ (July 9, 2025).

161. In addition, Plaintiff Weinberger seeks to represent all persons in the state of Florida who accessed CVS's digital or web-based properties, including, but not limited to the CVS Website, CVSHealth.com, and the CVS App while in Florida and had their Private Information intercepted, eavesdropped, and/or recorded by third parties (the "Florida Subclass").

162. In addition, Plaintiffs Brooks and Brewer seek to represent all persons in the state of California who accessed CVS's digital or web-based properties, including, but not limited to the CVS Website, CVSHealth.com, and the CVS App while in California and had their Private Information intercepted, eavesdropped, and/or recorded by third parties (the "California Subclass").

163. In addition, Plaintiff Sisti seeks to represent a class of all Maryland residents who accessed CVS's digital or web-based properties, including, but not limited to the CVS Website, CVSHealth.com, and the CVS App while in Maryland and had their Private Information intercepted, eavesdropped, and/or recorded by third parties (the "Maryland Subclass") (all collectively, the "Classes").

164. Members of the Classes are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Classes number in the millions. The precise number of Class Members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Class Members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendants.

165. Common questions of law and fact exist as to all Class Members and predominate over questions affecting only individual Class Members. Common legal and factual questions include, but are not limited to, whether Defendants violated the ECPA, FSCA, CIPA, or the Maryland Wiretap Act, whether Defendants invaded Plaintiffs' and Class Members' privacy and

breached their confidence, and whether Class Members are entitled to actual and/or statutory damages for the aforementioned violations.

166. The claims of the named Plaintiffs are typical of the claims of the Classes because the named Plaintiffs, like all other Class Members, accessed the Application and/or Website and had their electronic communications related to their Private Information intercepted by the Third-Party Trackers through CVS' employment of Third-Party Trackers' services.

167. Plaintiffs are adequate representatives of the Classes because their interests do not conflict with the interests of the Class Members they seek to represent, they have retained competent counsel experienced in prosecuting class actions, and they intend to prosecute this action vigorously. The interests of Class Members will be fairly and adequately protected by Plaintiffs and their counsel.

168. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class Members. 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 Defendants' 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 Defendants' 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.

CAUSES OF ACTION

COUNT I
Violation of the Federal Wiretap Act
18 U.S.C. § 2510, *et seq.*

169. Plaintiffs hereby incorporate by reference the allegations contained in paragraphs 1 through 165 above as if fully stated herein.

170. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents of any wire, oral, or electronic communications through the use of a device. 18 U.S.C. § 2511.

171. The Federal Wiretap Act protects both the sending and receiving of communications.

172. 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.

173. The transmissions of Plaintiffs' Private Information to the Website and/or Application qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

174. **Electronic Communications.** The transmission of Private Information between Plaintiffs and Class Members on one hand, and CVS on the other hand, with which they chose to exchange communications, are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

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

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

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

a. Plaintiffs' and Class Members' browsers;

a. Plaintiffs' and Class Members' computing and/or mobile devices;

b. CVS' webservers; and

c. The Third-Party Trackers' software deployed by CVS to effectuate the sending and acquisition of patient communications.

178. By utilizing and embedding the Third-Party Trackers' software on the Website and/or Application, CVS intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

179. Additionally, Defendant Criteo intentionally intercepted and endeavored to intercept the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

180. Specifically, through CVS' action of embedding the Third-Party Trackers' software on the Website and Application, which CVS knew would track, store, and unlawfully transmit Plaintiffs' and Class Members' Private Information to third parties, CVS procured the Third-Party

Trackers, to intercept Plaintiffs' and Class Members' electronic communications. *See* 18 U.S.C. § 2511(1)(a).

181. The communications CVS allowed to be intercepted include, but are not limited to, communications to/from Plaintiffs and Class Members regarding their Private Information.

182. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to third parties in the manner alleged herein, 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), Defendants violated 18 U.S.C. § 2511(1)(c).

183. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members for analytics and marketing purposes, 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), Defendants violated 18 U.S.C. § 2511(1)(d).

184. **Unauthorized Purpose.** CVS intentionally intercepted, and procured third parties to intercept or endeavor to intercept, the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the laws of the United States or of any State – namely, violation of the ECPA and HIPAA described herein.

185. CVS intentionally used the wire or electronic communications to increase profit margins for CVS. For instance, CVS specifically used the Third-Party Tracking software to track and utilize Plaintiffs' and Class Members' Private Information for CVS' financial gain including but not limited to using the tracked Private Information to target Plaintiffs and Class Members with advertisements for marketing and retargeting purposes.

186. CVS was not acting under color of law to intercept or procure the third parties, to intercept or endeavor to intercept, Plaintiffs and Class Members' wire or electronic communications.

187. Plaintiffs and Class Members did not authorize Defendants to acquire the content of their communications for purposes of invading Plaintiffs' privacy by transmitting their Private Information via the Third-Party Trackers' technology or any other third-party platforms.

188. Any purported consent that Defendants received from Plaintiffs and Class Members was not valid.

189. In transmitting, acquiring, and procuring third parties, to intercept or endeavor to intercept, the content of Plaintiffs' and Class Members' communications relating to the browsing of the Website and/or Application, CVS' purpose was tortious, criminal, and designed to violate federal and state legal provisions, including as described above the following: the ECPA and HIPAA.

COUNT II
Violation of the Florida Security of Communications Act
Fla. Stat. § 934.03 *et seq.*
(On Behalf of Plaintiff Weinberger and the Florida Subclass)

190. Plaintiffs hereby incorporate by reference the allegations contained in paragraphs 1 through 165 above as if fully stated herein.

191. Plaintiff Weinberger brings this claim against Defendants individually and on behalf of the Florida Subclass.

192. Fla. Stat. § 934.03(1) imposes liability on any person who (a) "[i]ntentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication"; (b) "[i]ntentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to

intercept any oral communication" when the device is "affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication" or "transmits communications by radio or interferes" with the transmission of the communication; (c) "[i]ntentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or (d) "[i]ntentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection[.]" Fla. Stat. § 934.03(1).

193. As used in the FSCA, "intercept" means the "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).

194. "Contents" when "used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." Fla. Stat. § 934.02(7).

195. The FSCA defines "electronic communication" as "[a]ny 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).

196. "Person" is defined as "any individual, partnership, association, joint stock company, trust or corporation." Fla. Stat. § 934.02(5).

197. Defendants are persons for purposes of the FSCA because they are corporations.

198. CVS contrived, agreed, conspired, effectuated, aided and/or procured the interception and use of the contents of Plaintiff Weinberger and Florida Subclass Members' communications by implementing the Third-Party Trackers on the Website and Application and configuring them in such as way that allowed the Third-Party Trackers to intercept Plaintiff Weinberger and Florida Subclass Members' Private Information.

199. The Third-Party Trackers; Plaintiff's and Florida Subclass Members' browsers; the Website; the Application; Plaintiff's and Class Members' computing and mobile devices; and CVS's servers and all qualify as a "device" under the FSCA.

200. CVS intentionally procured the Third-Party Trackers to intercept Plaintiff Weinberger and Florida Subclass Members' confidential and private communications, including their Private Information from the Website and/or Application.

201. Further, Medallia and Criteo intercepted the contents of these communications because each received the substance of these communications.

202. Defendants used, and allowed third parties to use, Plaintiff Weinberger's and Florida Subclass Members' confidential and private communications, including sensitive information, intercepted through the Third-Party Trackers.

203. The interception and use of Plaintiff Weinberger's and Florida Subclass Members' communications were without authorization and consent from Plaintiff and Florida Subclass Members.

204. Plaintiff Weinberger and Florida Subclass Members seek statutory damages in accordance with Fla. Stat. § 934.10(b), which provides for (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

205. Plaintiff Weinberger and Florida Subclass Members have also suffered irreparable injury from these unauthorized acts. Their personal, private, and sensitive personal information have been intercepted, viewed, accessed, stored, and used as a result of the Third-Party Trackers, and have not been destroyed, and due to the continuing threat of such injury, have no adequate remedy at law, Plaintiff Weinberger and Florida Subclass Members are entitled to injunctive relief.

COUNT III
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 631
(On Behalf of Plaintiffs Brooks and Brewer and the California Subclass)

206. Plaintiffs hereby incorporate by reference the allegations contained in paragraphs 1 through 165 above as if fully stated herein.

207. Plaintiffs Brooks and Brewer bring this claim against Defendants individually and on behalf of the California Subclass.

208. The California Legislature enacted the CIPA to protect certain privacy rights of California citizens. The 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.

209. The California Supreme Court has repeatedly stated an "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)

210. 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 (1985) (emphasis added; internal citations omitted).

211. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Super. Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> 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*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or 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*
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*
>
> 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.

212. CIPA § 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications.").

213. The Third-Party Trackers' software are a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

214. The Third-Party Trackers are "separate legal entit[ies] that offer[] 'software-as-a-service' and not merely [] passive device[s]." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Accordingly, the Third-Party Trackers were third parties to any communication between Plaintiffs and California Subclass Members, on the one hand, and CVS, on the other. *Id.* at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023); *Yoon*, 549 F. Supp. 3d at 1081.

215. At all relevant times, the Third-Party Trackers (including Defendant Criteo) willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiffs Brooks and Brewer and California Subclass Members on the one hand, and CVS, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

216. At all relevant times, Defendant aided, agreed with, employed, or otherwise enabled

the Third-Party Trackers to intercept consumers' communications with CVS and to accomplish the wrongful conduct at issue here.

217. The Third-Party Trackers' software is designed so that they transmit each of the user's actions taken on the Website and/or Application to the Third-Party Trackers contemporaneously with the user making the communications. Thus, the communications were intercepted while they were in transit to the intended recipient, CVS, and before they reached CVS's server, or while they were being sent from any place within California.

218. Plaintiffs Brooks and Brewer and California Subclass Members did not consent to the Third-Party Trackers' (including Defendant Criteo) intentional access, interception, reading, learning, recording, and collection of Plaintiffs Brooks and Brewer and California Subclass Members' electronic communications. Nor did Plaintiffs and California Subclass Members consent to CVS aiding, agreeing with, employing, or otherwise enabling the Third-Party Trackers' conduct.

219. Plaintiffs Brooks and Brewer and California Subclass Members seek all relief available under Cal. Penal Code § 637.2, including statutory damages of $5,000 per violation.

COUNT IV
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 632
(On Behalf of Plaintiffs Brooks and Brewer and the California Subclass)

220. Plaintiffs hereby incorporate by reference the allegations contained in paragraphs 1 through 165 above as if fully stated herein.

221. Plaintiffs Brooks and Brewer bring this claim against Defendants individually and on behalf of the California Subclass.

222. California Penal Code § 632 prohibits an entity from:

> intentionally and without the consent of all parties to a

> confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio.

223. The Third-Party Trackers' software are "electronic amplifying or recording device[s]."

224. At all times, the communications between Plaintiffs Brooks and Brewer and California Subclass Members, on the one hand, and CVS on the other, were confidential because the communications included medical, pharmaceutical, and personally identifiable information.

225. At all relevant times, CVS intentionally used the Third-Party Trackers' services to enable the Third-Party Trackers (including Defendant Criteo) to eavesdrop upon and record the confidential communications of Plaintiffs and California Subclass Members.

226. Additionally, at all relevant times, Criteo intentionally eavesdropped and/or recorded Plaintiffs Brooks and Brewer and California Subclass Members' communications with CVS for marketing purposes.

227. When communicating with CVS via the Website and/or Application, Plaintiffs Brooks and Brewer and California Subclass Members had an objectively reasonable expectation of privacy. Plaintiffs Brooks and Brewer and California Subclass Members did not reasonably expect that anyone other than CVS would be on the other end of the confidential communications, nor that other third-party entities like QM, Adobe, Criteo, and Medallia, would eavesdrop upon and record the confidential communications of Plaintiffs Brooks and Brewer and California Subclass Members. Indeed, Plaintiffs Brooks and Brewer and California Subclass Members each communicated medical-related information to CVS, which enhanced their reasonable expectation of privacy because such sensitive information should not be disclosed to nor intercepted by third

parties like the Third-Party Trackers.

228. Plaintiffs Brooks and Brewer and California Subclass Members did not provide their prior consent to the Third Party Trackers' intentional access, interception, reading, learning, recording, and collection of their electronic communications.

229. Plaintiffs Brooks and Brewer and California Subclass Members were in California when they accessed the Website and/or Application.

230. Pursuant to Cal. Penal Code § 637.2, Plaintiffs Brooks and Brewer and California Subclass Members have been injured by the violations of CIPA § 632(a), and seek statutory damages of $5,000 for each of Defendants' violations of CIPA § 632(a).

COUNT V
Violation of the California Invasion of Privacy Act, Trap and Trace Law
Cal. Penal Code § 638.51
(On Behalf of Plaintiffs Brooks and Brewer and the California Subclass)

231. Plaintiffs hereby incorporate by reference the allegations contained in paragraphs 1 through 165 above as if fully stated herein.

232. California's Trap and Trace Law is part of CIPA, codified at Cal. Penal Code 630, *et seq.*

233. A "trap and trace device" as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c).

234. California Penal Code § 638.51(a) provides that "a person may not install or use…a trap and trace device without first obtaining a court order . . . ."

235. At all relevant times, CVS used a trap and trace process on CVS's digital or web-based properties, including, but not limited to the CVS Website, CVSHealth.com, and the CVS

App by deploying technology that captures routing, addressing and/or other signaling information of website visitors including Plaintiffs Brooks and Brewer and California Subclass Members.

236. Plaintiffs Brooks and Brewer and California Subclass Members did not provide their prior consent to CVS using trap and trace technology to identify users of CVS's digital or web-based properties, including, but not limited to the CVS Website, CVSHealth.com, and the CVS App.

237. Plaintiffs Brooks and Brewer and California Subclass Members were in California when they accessed the Website and/or Application.

238. Pursuant to Cal. Penal Code § 637.2, Plaintiffs Brooks and Brewer and California Subclass Members have been injured by the violations of CIPA § 638.51 and seek statutory damages of $5,000 for each of Defendants' violations of CIPA § 638.51.

COUNT VI
Violation of the Maryland Wiretap Act
Md. Cts. & Jud. Pro. § 10-401 *et seq.*
(On Behalf of Plaintiff Sisti and the Maryland Subclass)

239. Plaintiffs hereby incorporate by reference the allegations contained in paragraphs 1 through 165 above as if fully stated herein.

240. Plaintiff Sisti brings this claim against Defendants individually and on behalf of the Maryland Subclass.

241. The Maryland Wiretap Act bars the surreptitious interception and recording of private communications. Md. Cts. & Jud. Pro. § 10-402.

242. It is a violation of the Maryland Wiretap Act for any person to "[w]illfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." *Id.* § 10-402(a)(1).

243. "Person" includes "any individual, partnership, association, joint stock company,

trust, or corporation." Md. Cts. & Jud. Pro. § 10-401(14).

244. Defendants, as corporations, are "persons" under the Maryland Wiretap Act.

245. "Intercept" is defined as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id*. § 10-401(10).

246. "Contents" is defined as either "any information concerning the identity of the parties to such communication," or any information concerning the "existence, contents, substance, purport, or meaning of that communication." *Id.* § 10-401(4).

247. "Electronic communication" is defined 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 photooptical system." *Id.* § 10-401(5)(i).

248. Defendants willfully employed the Tracking Technologies to automatically and indiscriminately transmit to Defendants Website users' confidential electronic communications to third parties as they take place in real time, in violation of § 10-402.

249. When communicating with CVS via the Website and/or Application, Plaintiff Sisti and Maryland Subclass Members had an objectively reasonable expectation of privacy. Plaintiff Sisti and Maryland Subclass Members did not reasonably expect that anyone other than CVS would be on the other end of the confidential communications, nor that other third-party entities like QM, Adobe, Criteo, and Medallia, would eavesdrop upon and record the confidential communications of Plaintiff Sisti and Maryland Subclass Members. Indeed, Plaintiff Sisti and Maryland Subclass Members communicated medical-related information to CVS, which enhanced their reasonable expectation of privacy because such sensitive information should not be disclosed to nor intercepted by third parties like the Third-Party Trackers.

250. Plaintiff Sisti and Maryland Subclass Members did not provide their prior consent to the Third Party Trackers' intentional access, interception, reading, learning, recording, and collection of their electronic communications.

251. Plaintiff Sisti and Maryland Subclass Members are each entitled to "[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, which is higher;" and punitive damages. Md. Cts. & Jud. Pro. § 10-403.

252. Plaintiff Sisti and Maryland Subclass Members are also entitled to a "reasonable attorney's fee and other litigation disbursements reasonably incurred." *Id*.

COUNT VII
Breach of Confidence

253. Plaintiffs hereby incorporate by reference the allegations contained in paragraphs 1 through 165 above as if fully stated herein.

254. Plaintiffs and Class Members disclosed in confidence their health and private information with CVS through the Website. Plaintiffs and Class Members have an interest in keeping their protected private and medical information in confidence with CVS.

255. The information Defendants disclosed and intercepted in confidence is protected health and private information Defendants had knowledge was confidential due, in part, to federal and state laws that protect such information (i.e., ECPA, HIPAA).

256. Plaintiffs and Class Members had an expectation that the confidential information they provided to CVS and intercepted by the Third-Party Trackers would be kept in confidence with CVS due to the sensitive nature of their relationship with CVS and communications concerning sensitive health issues and medical care.

257. Defendants violated their duty to not intercept and to protect the confidentiality of Plaintiffs' and Class Members' information by using the Tracking Technologies to communicate

and intercept patients' individually identifying information and confidential medical communications.

258. Defendants disclosed and intercepted Plaintiffs' and Class Members' confidential information for their own economic benefit and without Plaintiffs' and Class Members' knowledge or consent.

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

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

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

COUNT VIII
Invasion of Privacy—Intrusion Upon Seclusion

262. Plaintiffs hereby incorporate by reference the allegations contained in paragraphs 1 through 165 above as if fully stated herein.

263. Plaintiffs and Class Members had a reasonable expectation of privacy in communications with CVS via the Website and the communications platforms and services therein.

264. Plaintiffs and Class Members communicated sensitive and protected medical information and individually identifiable information that they intended for only CVS to receive and that they understood would be kept private.

265. Defendants' disclosure and interception of the substance and nature of those

communications as described above without the knowledge and consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion.

266. Plaintiffs and Class Members had a reasonable expectation that their communications, identity, health information, and other data would remain confidential and that Defendants would not secretly disclose and intercept their communications as described above.

267. CVS was authorized to obtain Private Information from Plaintiffs and Class Members for itself but was not authorized to force Plaintiffs' and Class Members' web browsers to transmit information to the Third-Party Trackers without their consent or authorization. Likewise, the Third-Party Trackers were not authorized to intercept Plaintiffs' and Class Members' private communications with CVS.

268. Defendants therefore obtained Plaintiffs' and Class Members' Private Information under false pretenses and/or exceeded their authority to obtain the Private Information.

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

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

271. 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 Defendants' intrusions upon Plaintiffs' and Class Members' privacy.

272. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendants' actions, directed at injuring Plaintiffs

and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendants from engaging in such conduct in the future.

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

COUNT IX
Negligence and Negligence *Per Se*

274. Plaintiffs hereby incorporate by reference the allegations contained in paragraphs 1 through 165 above as if fully stated herein.

275. Plaintiffs and Class Members entrusted their sensitive and protected medical information and individually identifiable information to CVS.

276. Defendants had a duty to safeguard and not disclose or intercept Plaintiffs' and Class Members' sensitive and protected medical information and individually identifiable information as described above without Plaintiffs' knowledge or consent.

277. CVS also maintained a duty to safeguard and Plaintiffs' and Class Members' sensitive and protected medical information and identifiable information under their obligations to protect personally identifying health information as outlined by applicable laws and regulations, including but not limited to the statutory obligations for HIPAA and regulations from HHS.

278. The Third-Party Trackers likewise also maintained a duty to maintain the privacy of Plaintiffs' and Class Members' sensitive and protected medical information when working with CVS to intercept their communications.

279. Defendants could have configured the Adobe Trackers to not record, track, and transmit Plaintiffs' and Class Members' sensitive and protected medical information and individually identifiable information.

280. Defendants breached their duty to maintain the privacy of Plaintiffs' and Class Members' sensitive and protected medical information and individually identifiable information

disclosed and intercepted communications containing this information without Plaintiffs' and Class Members' knowledge or consent, as described above.

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

282. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendants' negligence and are entitled to just compensation, including monetary damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendants, as follows:

(a) For an order certifying the Classes under Rule 23, naming Plaintiffs as the representatives of the Classes, and naming Plaintiffs' attorneys as Class Counsel to represent the Classes;

(b) For an order declaring that the Defendants' conduct violates the ECPA;

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

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

(e) For pre- and post-judgment interest on all amounts awarded; and

(f) For an order awarding Plaintiffs and the Classes their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Pursuant to Federal Rules of Civil Procedure 38(b), Plaintiffs demand a trial by jury of all issues so triable.

Dated: July 24, 2026

By: */s/ Jeff Ostrow*

Jeff Ostrow FBN 121452
KOPELOWITZ OSTROW P.A.
1 W Las Olas Blvd, Suite 500
Ft. Lauderdale, FL 33301
Telephone: (954) 525-4100
ostrow@kolawyers.com

Mariya Weekes FBN 56299
MILBERG, PLLC
333 SE 2nd Avenue, Suite 2000
Miami, FL 33131
Telephone: (866) 252-0878
mweekes@milberg.com

Jonathan M. Jagher (*pro hac vice* pending)
JUSTICE JAGHER LONDON & MILLEN LLC
923 Fayette St.
Conshohocken, PA 19428
Telephone: (224) 632-4500
Facsimile: (224) 632-4521
jjagher@jjlmlaw.com

Katrina Carroll (*pro hac vice* forthcoming)
CARROLL SHAMBERG LLC
111 W. Washington Street
Suite 1240
Chicago, IL 60602
Tel. 872-215-6205
katrina@csclassactions.com

Yitzchak Kopel (*pro hac vice* forthcoming)
BURSOR & FISHER, P.A.
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-1750
Facsimile: (212) 989-9163
ykopel@bursor.com

Counsel for Plaintiffs and the Putative Class

Public court record.

This copy was downloaded from https://cw.simpluris.com/docs/public/downloads/CBC4/AMENDED_C
on 2026-11-02 and is hosted, unaltered, for reference at
https://chimo.ai/class-action/cvs-digital-privacy

Court: Circuit Court of the 17th Judicial Circuit, Broward County, Florida
Case number: CACE-26-008094

Chimo hosts public court records for readers' reference; documents are
unaltered copies from the court docket or the court-approved settlement website.