JS 44 (Rev. 10/20)

CIVIL COVER SHEET

County in which action arose: Wayne

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Bruce W. Falls, Margaret Jean Ciolek Fay, Elliott A. Davis, Craig Diegel, Kathy Morren, individually and on behalf of all others similarly situyated,

(b) County of Residence of First Listed Plaintiff Shelby County, Alabama
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
R.J. Cronkhite, Cronkhite Counsel PLLC, 36800 Woodward Ave., Ste. 310, Bloomfield Hills, MI 48304, (248) 309-8601; Andrew D. Schlichter, Schlichter Bogard LLC, 100 S. 4th Street, Ste. 1200, St. Louis, MO 63102, (314) 621-6115

DEFENDANTS

Blue Cross Blue Shield of Michigan Mutual Insurance Company,

County of Residence of First Listed Defendant Wayne
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ■ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	■ 4
Citizen of Another State	■ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 422 Appeal 28 USC 158	☐ 375 False Claims Act
☐ 120 Marine	☐ 310 Airplane	☐ 365 Personal Injury - Product Liability	☐ 690 Other	☐ 423 Withdrawal 28 USC 157	☐ 376 Qui Tam (31 USC 3729(a))
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	☐ 400 State Reapportionment
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability		☐ 820 Copyrights	☐ 410 Antitrust
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	☐ 830 Patent	☐ 430 Banks and Banking
☐ 151 Medicare Act	☐ 340 Marine	☐ 370 Other Fraud	☐ 710 Fair Labor Standards Act	☐ 835 Patent - Abbreviated New Drug Application	☐ 450 Commerce
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 720 Labor/Management Relations	☐ 840 Trademark	☐ 460 Deportation
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 740 Railway Labor Act	☐ 880 Defend Trade Secrets Act of 2016	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	☐ 751 Family and Medical Leave Act	SOCIAL SECURITY	☐ 480 Consumer Credit (15 USC 1681 or 1692)
☐ 190 Other Contract	☐ 360 Other Personal Injury		☐ 790 Other Labor Litigation	☐ 861 HIA (1395ff)	☐ 485 Telephone Consumer Protection Act
☐ 195 Contract Product Liability	☐ 362 Personal Injury - Medical Malpractice		☐ 791 Employee Retirement Income Security Act	☐ 862 Black Lung (923)	☐ 490 Cable/Sat TV
☐ 196 Franchise				☐ 863 DIWC/DIWW (405(g))	☐ 850 Securities/Commodities/ Exchange
				☐ 864 SSID Title XVI	■ 890 Other Statutory Actions
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION	☐ 865 RSI (405(g))	☐ 891 Agricultural Acts
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	**Habeas Corpus:**	☐ 462 Naturalization Application		☐ 893 Environmental Matters
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee	☐ 465 Other Immigration Actions	FEDERAL TAX SUITS	☐ 895 Freedom of Information Act
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence		☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 896 Arbitration
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General		☐ 871 IRS—Third Party 26 USC 7609	☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 535 Death Penalty			☐ 950 Constitutionality of State Statutes
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	**Other:**			
	☐ 448 Education	☐ 540 Mandamus & Other			
		☐ 550 Civil Rights			
		☐ 555 Prison Condition			
		☐ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

■ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
18 U.S.C. § 2510 et seq., 28 U.S.C. § 1332(d)(2)(A)

Brief description of cause:
Federal Wiretap Act, Michigan Eavesdropping Statute (MCL 750.539h), Breach of Fiduciary Duty, Intrusion Upon Seclusion, Unjust Enrichment

VII. REQUESTED IN COMPLAINT:

■ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ >$5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ■ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
December 31, 2025

SIGNATURE OF ATTORNEY OF RECORD
/s/ R.J. Cronkhite (P78374)

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

PURSUANT TO LOCAL RULE 83.11

1. Is this a case that has been previously dismissed?

☐ Yes
☒ No

If yes, give the following information:

Court: _____

Case No.: _____

Judge: _____

2. Other than stated above, are there any pending or previously discontinued or dismissed companion cases in this or any other court, including state court? (Companion cases are matters in which it appears substantially similar evidence will be offered or the same or related parties are present and the cases arise out of the same transaction or occurrence.)

☐ Yes
☒ No

If yes, give the following information:

Court: _____

Case No.: _____

Judge: _____

Notes :

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

BRUCE W. FALLS, MARGARET JEAN CIOLEK FAY, ELLIOTT A. DAVIS, CRAIG DIEGEL, KATHY MORREN, individually and on behalf of all others similarly situated, *Plaintiffs*, v. BLUE CROSS BLUE SHIELD OF MICHIGAN MUTUAL INSURANCE COMPANY, *Defendant*.	Civil Action No. **JURY DEMANDED**

CLASS ACTION COMPLAINT

1. Plaintiffs Bruce W. Falls, Margaret Jean Ciolek Fay, Elliott A. Davis, Craig Diegel, and Kathy Morren ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this class action lawsuit against defendant Blue Cross Blue Shield of Michigan Mutual Insurance Company for violations of the Federal Wiretap Act, 18 U.S.C. § 2510 et seq. ("FWA"), Michigan's eavesdropping statute, MCL 750.539a et seq., as well as for breach of fiduciary duty, intrusion upon seclusion, and unjust enrichment. Plaintiffs allege the following facts

based upon personal knowledge, investigation by counsel, and information and belief.

2. Defendant wiretapped its insureds in a brazen and invasive betrayal of trust. Defendant harvested highly sensitive health-related information from its insureds using hidden tracking tools and secretly disseminated this private health-related information to third parties.

3. Plaintiffs were not notified of Defendant's hidden tracking and harvesting of their private information, which began as soon as Plaintiffs loaded Defendant's www.bcbsm.com website. Nor were Plaintiffs provided an opportunity to limit, or consent to, Defendant's tracking and harvesting of their personal health information.

4. Defendant's public-facing representations about its privacy practices were inadequate and affirmatively misleading, including because Defendant represented that no disclosure of Plaintiffs' private information would occur for marketing or other similar purposes, and that no disclosure of Plaintiffs' private information would occur absent Plaintiffs' express written permission. Yet, Defendant surreptitiously tracked and disseminated Plaintiffs' private health-related information, disseminating this information to third parties including Verint

Systems, Inc. ("Verint"), Adobe Inc. ("Adobe"), Datadog, Inc. ("Datadog"), and Qualtrics, LLC ("Qualtrics").

5. Even within Defendant's purportedly secure patient portals – where insureds access claims, review prescriptions (for specific medications in specific dosages), and review information concerning sensitive medical conditions with tools designed to help identify ailments – Defendant's surreptitious tracking of Plaintiffs' private health-related information was constant and pervasive, and the highly sensitive health-related data of Plaintiffs and other insureds were transmitted, in real time, to third parties without any form of consent.

6. Plaintiffs seek damages and injunctive relief to redress Defendant's unlawful interception and misuse of their private health-related information.

NATURE OF THE CASE

A. Defendant's Interception of Website and Portal Communications

7. This action challenges Defendant's practice of surreptitiously intercepting and misusing personal, highly sensitive health-related information from the www.bcbsm.com website, portals, and other pages

on the bcbsm.com website like the prescription portal or LiveWell information pages (together with subpages, Defendant's "Website").

8. Defendant has violated, and continues to violate, the FWA, Michigan's eavesdropping statute, and Michigan common law by wiretapping the electronic health-related communications of Plaintiffs and Defendant's insureds on Defendant's Website.

9. Defendant's violations occur as follows: Entirely unbeknownst to insureds, third-party vendors – including Verint, Adobe, Datadog, and Qualtrics (collectively, "Third-Party Vendors") – have supplied tracking technologies ("Tracking Pixels" and "Session Replay Code," or "Tracking Technologies") to Defendant, which Defendant has embedded on its Website.

10. These Tracking Technologies load immediately on both public-facing pages of Defendant's Website, and within purportedly secure portals, to covertly track, intercept, and record insureds' communications with Defendant, including but not limited to insureds' keystrokes (i.e., text entered into a search box or information box), web addresses (i.e., "URLs") of individual pages visited, mouse movements,

clicks, and/or other electronic communications in real time ("Website Communications").

11. After surreptitiously intercepting and capturing the Website Communications of insureds, Defendant and the Third-Party Vendors use these Website Communications for purposes that benefit and enrich themselves to the detriment of insureds.

12. The Third-Party Vendors use the harvested personal health-related information they obtain to create and/or bolster advertising profiles of insureds, to target or retarget advertisements to insureds, and/or to sell information about insureds to other entities for commercial gain.

13. Defendant uses the harvested information to track visits to Defendant's Website, allowing them to covertly recreate insureds' entire sessions on Defendant's Website. This includes detailed replays of portal sessions, the exact prescriptions and dosages taken by insureds, provider or treatment searches, or even specific research by Plaintiffs on LiveWell pages that discuss specific medical issues.

14. Defendant also uses the embedded Tracking Technologies that load immediately once an insured accesses the Website to create a replay of their behavior on the Website.

15. This collection of insureds' highly sensitive, private data takes place without notice to or consent from insureds.

16. Defendant causes the collection of this highly sensitive, private data by embedding the code of the Tracking Technologies, such as Tracking Pixels, in the Website. This embedded code instantly sends private health-related data to Third-Party Vendors.

17. Defendant thereby permits the Third-Party Vendors to intercept insureds' private healthcare data.

18. Defendant also benefits financially by obtaining and analyzing insureds' private healthcare data that enables them to add new customers, replacing the need for (and costs associated with) advertising and surreptitiously finding targets for advertising campaigns.

19. These commercial advantages come at the expense of insureds' privacy and contradict Defendant's online promises to safeguard health-related information and legal duty to do the same.

B. Defendant's Legal Duties and Resulting Harms

20. Defendant's violations have broad-ranging deleterious effects because Defendant holds highly sensitive, personal health-related data of its insureds. These data include private medical and health information, as well as related unique personal identifiers, health details, and other data provided by insureds related to or for the purpose of obtaining healthcare.

21. Federal privacy laws require robust privacy protections for these highly sensitive, personal health-related data.

22. Defendant is a covered entity under the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1320d et seq., because it operates numerous health plans nationwide and meets the statutory and regulatory requirements of a health plan. *See* 45 C.F.R. § 160.103.

23. A business associate is an entity that performs activities on behalf of, or provides services to, a covered entity involving the use or disclosure of protected health information ("PHI"). *See* 45 C.F.R. § 160.103.

24. Defendant is also a business associate because it performs services involving PHI on behalf of covered entities, including its health plan subsidiaries. These services include, but are not limited to, data analysis and reporting, claims administration, member communication or outreach, and other reviews.

25. Under HIPAA, a covered entity or business associate must comply with HIPAA privacy and security rules with respect to individually identifiable health information, or "IIHI." *See* 45 C.F.R. §§ 164.302–316; 164.500–534.

26. Covered entities and business associates are required to implement administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of PHI. 45 C.F.R. § 164.306.

27. Covered entities and business associates are prohibited from using or disclosing PHI except as permitted by law. *See* 45 C.F.R. §§ 164.502(a)(3); 164.504(e).

28. Disclosure of PHI for marketing or analytics purposes – such as to data brokers or advertising networks – is explicitly prohibited absent valid, written authorization. *See* 45 C.F.R. § 164.508(a)(3)

(noting that "a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing"); *id.* § 164.508(c)(1)(vi).

29. Defendant acts as a fiduciary with respect to the sensitive data that it collects and manages on behalf of Plaintiffs.

30. By designing, operating, and maintaining the Website through which Plaintiffs access password-protected health benefit information, Defendant assumes the responsibility and duty to safeguard these data and use them solely for authorized, health-related purposes.

31. This fiduciary duty includes a duty of loyalty and care, requiring Defendant to avoid exploiting Plaintiffs' data for commercial benefit or disclosing data to third parties like the Third-Party Vendors without clear, informed, and express consent.

32. As a result of Defendant's violations and invasions of the privacy rights of its insureds, these insureds, including Plaintiffs, have suffered significant harms, including but not limited to a loss of privacy and control over their private health-related data, greatly increased vulnerability to identity theft and fraud, and the surreptitious use of

their confidential financial and health-related information for the benefit of Defendant and others, without any consent.

33. Plaintiffs bring this action individually and on behalf of a nationwide class of all insureds of Defendant whose Website Communications were wiretapped and intercepted via the code embedded on Defendant's Website.

34. Plaintiffs seek all civil remedies provided under the below causes of action, including but not limited to compensatory, statutory, treble, punitive damages, and attorneys' fees and costs.

PARTIES

A. Plaintiffs.

35. Plaintiff Bruce W. Falls, former policeman and U.S. Army veteran, is a resident of Shelby in Shelby County, Alabama. He was insured under a health policy of Defendant through his employer, Yellow Corporation, from 1985 to 2023. After working for Yellow Corporation, he purchased his own policy through Defendant, which he retained for approximately one year before relocating to Alabama and switching insurers. During the relevant time period (December 2023 to the present), he accessed Defendant's Website.

36. Plaintiff Margaret Jean Ciolek Fay is a resident of Ada in Kent County, Michigan. She has been insured under a health policy of Defendant through her employer, SAF Holland, for the past four years. During the relevant time period, she routinely used Defendant's Website for various purposes. Her two children were also insureds, and Ms. Fay used the Website in connection with overseeing their health care.

37. Plaintiff Elliott A. Davis is a resident of Wixom in Oakland County, Michigan. For the past several years, he has been insured under a Medicare Advantage health policy of Defendant. During the relevant time period, he routinely used Defendant's Website in connection with his health-care needs.

38. Plaintiff Craig Diegel is a resident of Clinton Township in Macomb County, Michigan. He has been insured under a health policy of Defendant through his employer since October of 2024. During the relevant time period, he routinely used Defendant's Website in connection with his health-care needs.

39. Plaintiff Kathy Morren is a resident of Chase in Lake County, Michigan. She has been insured under a health policy of

Defendant for over 30 years. During the relevant time period, she routinely used Defendant's Website in connection with her health-care needs.

B. Defendant BCBSM.

40. Defendant is a health insurer and an independent licensee of the Blue Cross Blue Shield Association.[1]

41. Defendant is headquartered in Detroit, Michigan.[2]

42. Defendant operates as a nonprofit mutual insurance company under Chapter 58 of the Michigan Insurance Code, providing individual, small-group, and Medicare supplemental products.[3]

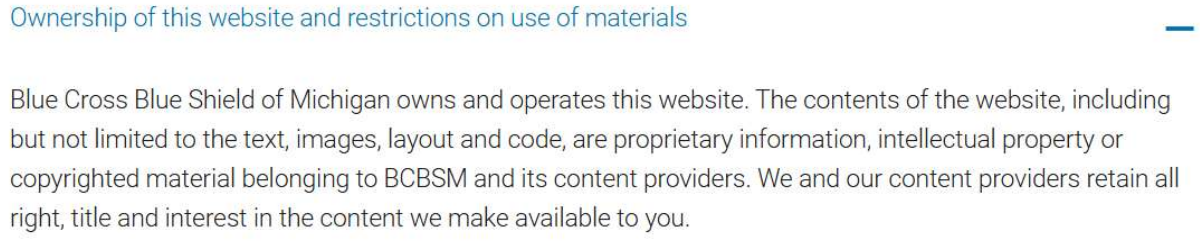
43. Defendant serves approximately 4.5 million insureds, primarily in the state of Michigan.[4]

44. In 2023, Defendant had the thirteenth largest market share of all U.S. health insurance carriers, capturing approximately 1.2% of

[1] *Fast Facts*, BCBSM, https://www.bcbsm.com/about-us/our-company/fast-facts/ [https://perma.cc/52GW-X6XA].
[2] *Id.*
[3] *Notes to Consolidated Financial Statements as of and for the Years Ended December 31, 2021 and 2020* (2022), at 10, BCBSM MUTUAL INSURANCE CO., https://www.bcbsm.com/amslibs/content/dam/public/bcbsm/about/documents/2021-BCBSM-financial-statement.pdf [https://perma.cc/XX39-UVM2].
[4] *Building Trust*, BCBSM, https://buildingtrust.org/partner/blue-cross-blue-shield-of-michigan/ [https://perma.cc/N4AJ-U4XH].

the U.S. health insurance market. It wrote about $18.24 billion in net premiums in 2023.[5]

45. Defendant administers its Website through which insureds, such as Plaintiffs, access their health plan information:


Ownership of this website and restrictions on use of materials

Blue Cross Blue Shield of Michigan owns and operates this website. The contents of the website, including but not limited to the text, images, layout and code, are proprietary information, intellectual property or copyrighted material belonging to BCBSM and its content providers. We and our content providers retain all right, title and interest in the content we make available to you.

Figure 1[6]

46. Defendant is a "person" as defined in the FWA. 18 U.S.C. § 2510(6).

47. Defendant is a "person" as defined in Michigan's eavesdropping statute. MCL 750.539a(4).

JURISDICTION

48. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because Plaintiffs assert claims arising under the FWA, 18 U.S.C. §§ 2510–2523.

---

[5] Elizabeth Walker, *Top 25 Health Insurance Companies in the U.S.*, PEOPLEKEEP (Jan. 9, 2025), https://www.peoplekeep.com/blog/top-25-health-insurance-companies-in-the-u.s [https://perma.cc/QC8H-FFCA].

[6] *Terms & Conditions*, BCBSM, https://www.bcbsm.com/important-information/terms-conditions/ [https://perma.cc/4GEX-KV5R].

49. This Court also has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2)(A) because this is a class action in which the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs; there are 100 or more members of the proposed class; and at least one member of the proposed class, inclusive of Plaintiffs, is a citizen of a different state than Defendant.

50. Jurisdiction in this District is neither arbitrary nor inconvenient for Defendant, as it is where it is headquartered and conducts substantial business with millions of insureds.

A. The Federal Wiretap Act.

51. Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the Federal Wiretap Act, to protect the privacy of wire, oral, and electronic communications from unauthorized interception, disclosure, and use. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 801-804, 82 Stat. 197, 211–25.

52. In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA") to amend the FWA in order to protect the privacy of electronic communications. Pub. L. No. 99-508, 100 Stat. 1848.

53. The ECPA was enacted to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. Rep. No. 99-541, at 1 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3555.

54. Title I of the ECPA amended the FWA to expand its coverage beyond wire and oral communication and to "address[ ] the interception of . . . electronic communications." S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557.

55. The "paramount objective of the [ECPA] is to protect effectively the privacy of communications."[7]

56. The FWA defines "person" to include "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

[7] *Joffe v. Google*, 746 F.3d 920, 931 (9th Cir. 2013) (quoting *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 18 (1st Cir. 2003)).

57. The FWA prohibits any "person" from (1) intentionally intercepting, endeavoring to intercept, or procuring another person to intercept or endeavor to intercept any wire, oral, or electronic communication; (2) intentionally disclosing, or endeavoring to disclose, the contents of any such communication knowing or having reason to know it was unlawfully intercepted; or (3) intentionally using, or endeavoring to use, the contents of any such communication knowing or having reason to know it was unlawfully intercepted. 18 U.S.C. § 2511(1).

58. The FWA, as amended by the ECPA, defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system. . ." 18 U.S.C. § 2510(12).

59. The term "contents," with respect to communications, includes "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

60. The FWA provides a civil cause of action to "[a]ny person whose wire, oral, or electronic communication is intercepted, disclosed,

or intentionally used in violation of this chapter" against the person or entity who engaged in such conduct. 18 U.S.C. § 2520(a).

61. The FWA permits recovery of preliminary and permanent injunctive relief, the greater of actual damages or statutory damages calculated at $100 per day or $10,000 per violation, punitive damages, and attorneys' fees and costs. 18 U.S.C. § 2520(b).

62. Although the FWA includes an exception permitting interception with the consent of "one of the parties to the communication," this exception does not apply where the interception is done "for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State" (commonly known as the "crime-tort exception"). 18 U.S.C. § 2511(2)(d). Here, Defendant intentionally deployed Tracking Technologies to intercept Website Communications for the unlawful purpose of disclosing PHI.

B. Michigan's Eavesdropping Statute.

63. The FWA allows states to "grant greater, but not lesser, protection than that available under federal law."[8]

[8] *Commonwealth v. Spangler*, 570 Pa. 226, 232, 809 A.2d 234, 237 (2002).

64. Michigan's eavesdropping statute, MCL 750.539a et seq., prohibits the unauthorized use of devices to overhear, record, transmit, or intercept private conversations.

65. Section 750.539c makes it unlawful for any person to "willfully use any device to eavesdrop upon the private conversation of others without the consent of all parties thereto."

66. Under the statute, "eavesdrop" is defined broadly, and means "to overhear, record, amplify or transmit any part of the private discourse of others without the permission of all persons engaged in the discourse." MCL 750.539a(2).

67. "Private conversation" includes any communication in which the participants reasonably expect "to be free from casual or hostile intrusion or surveillance."[9]

68. The statute is a "two-party consent" law, meaning that the consent of *all* participants is required before recording or interception may lawfully occur by *non-participants*. MCL 750.539c, 750.539e.

69. "When a third party is unilaterally given permission to listen in upon a conversation, unknown to other participants, those other

[9] *People v. Stone*, 463 Mich. 558, 563 (Mich. 2001).

participants are no longer able to evaluate and form accurate expectations since they are without knowledge of the third party."[10]

70. Liability under Michigan's eavesdropping statute attaches at the moment of interception, or when the recording, overhearing, or transmission by a third party occurs.

71. Michigan's eavesdropping statute provides for a private right of action under MCL 750.539h, and any person who has been injured by a violation of Michigan's eavesdropping statute is entitled to an injunction prohibiting further eavesdropping, to recover actual damages, and to recover punitive damages together with reasonable attorneys' fees and costs of litigation.

FACTUAL ALLEGATIONS

I. How Websites Can Use Code to Harvest Users' Private Information

A. Websites Can Be Used to Harvest Personal Data from Users.

72. Web browsers are software applications that allow users to navigate the Internet and view and exchange electronic information and communications.

[10] *Sullivan v. Gray*, 117 Mich. App. 476, 482 (1982).

73. Each "device" (such as a computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

74. Websites are hosted on servers, which are computers that store the site's data and facilitate the exchange of information between the website and the users' browsers.

75. Websites have domains, which are the human-readable name of the website, or what someone types into a browser to get to the site – with examples like google.com.

76. An HTTP request is a message sent from a web browser to a website's server to ask for information, such as loading a webpage or submitting a query.

77. An HTTP response is the message that a website's server sends in response to an HTTP request to the browser. It includes the requested information.

78. Web interactions involve HTTP requests and HTTP responses, with each browsing session typically involving thousands of these exchanges.

79. When a user visits a website, the website sends a small amount of data, known as a "cookie," to be stored on the user's browser.

80. Cookies are then stored locally on the user's browser and included with future requests to the same server.

81. Cookies are used to "remember" users between sessions, including how users interact with the website.

82. When users log into a website and it "remembers" them, it is often because of a cookie.

83. When a user visits a website, the browser sends an HTTP request to the server, requesting specific information – for example, the "Find Care" menu on Defendant's Website.

84. The server responds with an HTTP response, which includes the requested data in the form of "markup."

85. This markup is the underlying structure for what the user sees on the webpage, such as text, images, and interactive elements.

86. Websites are built using this markup and "source code," which provides instructions to the browser, dictating how the page behaves when it loads or when a particular action occurs.

87. Source code may be written to include instructions to send data to third parties via background HTTP requests.

88. Users may be unaware that data are being sent to third parties via requests.

89. These background requests can be designed to function like a digital wiretap, capturing and transmitting communications and facilitating the covert harvesting of consumer data.

90. Source code may also be written to send user data outward.

91. This source code can send information – like searches or messages – from the user's browser to the website's server.

92. When source code is written to send data requests to third-party domains and servers (especially in real time), the third parties receive data that users may not have intended to disclose.

B. Tracking Pixels and Session Replay Code Can Be Used to Extract Individuals' Private Information.

93. Tracking Pixels include a broad range of HTML and JavaScript code embedded in websites and emails.[11]

94. Tracking Pixels are hidden from sight.

[11] *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FTC (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking [https://perma.cc/Y8TJ-53FD].

95. Tracking Pixels trigger a network traffic request to the tracking entity's remote server.

96. By triggering this network traffic request, Tracking Pixels can track, collect, and send to third parties various private and/or personal data, such as how the user interacts with the website or information typed into text fields.[12]

97. Because Tracking Pixels embedded into websites such as Defendant's Website operate silently in the background, users often do not realize that their private and personal data are being collected as they browse the website.[13]

98. Tracking Pixels may collect various types of information, including sensitive information.

99. Some Tracking Pixels harvest data regarding website users' entertainment or shopping habits and preferences.

100. In this case, the Tracking Pixels embedded on Defendant's Website do not merely collect shopping trends or similar commercial

[12] *Id.*
[13] *Id.*

data; instead, Defendant's Tracking Pixels collect highly sensitive, personal, and private health-related information.

101. Session Replay Code operates similarly to Tracking Pixels, often relying on network traffic requests to transmit recorded interaction data.

102. However, Session Replay Code extracts even more intrusive details about users' browsing behavior.

103. Specifically, Session Replay Code logs and tracks *everything* a user does on a webpage, including mouse movements, clicks, scrolls, and taps, and can actually track every single key stroke, creating a *complete* reproduction of the user's visit to the website.[14]

104. Tracking Technologies also often use requests to send user data back to third-party servers.

II. Confidential Personal Heath Data Covertly Obtained from Websites Presents Serious Privacy Risks.

105. Data pertaining to individuals are so valuable they have been compared to the "new oil."[15]

---

[14] *The definitive guide to session replay*, Fullstory (Oct. 8, 2024), https://www.fullstory.com/blog/session-replay/ [https://perma.cc/56WH-8GQ5].
[15] *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/US3V-CPCU].

106. However, the market for such data, and in particular personal health-related data, presents serious privacy risks.

107. For this reason, Time Magazine has pointed out that the health data market, while highly lucrative, poses a significant risk to individuals' privacy.[16]

108. Nevertheless, the enormous value of personal health data incentivizes businesses to use invasive tracking technologies on their websites to collect these data from website users.

109. For example, the data collected by Tracking Pixels is valuable to businesses because they can use it to track Internet users and target ads based on prior browsing behavior.[17] This practice can be highly lucrative.

110. As one report explained, "There's a whole market of brokers who compile the [personal health] data from providers and other health-care organizations and sell it to buyers."[18]

---

[16] Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, TIME (Jan. 9, 2017), https://time.com/4588104/medical-data-industry/ [https://perma.cc/F3WR-HHVL].
[17] *Id.*
[18] Christina Farr, *Hospital Execs Say They are Getting Flooded with Requests for Your Health Data*, CNBC (Dec. 18, 2019, 8:27 AM), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html [https://perma.cc/D7CL-N3HX].

111. According to a report from cybersecurity company Feroot Security, "medical-related websites continue to be mined for data including personal medical information[.]"[19]

112. As early as 2015, experts were researching how confidential health information is shared with third parties without users' knowledge.[20]

113. In June 2022, an investigation by The Markup[21] revealed that one Tracking Pixel, the Meta Pixel, collected and sent a "data packet" to Facebook whenever a user engaged with some hospital websites, such as clicking to schedule a doctor's appointment.

114. Further research by The Markup revealed that the personal health data transmitted to Facebook by the Meta Pixel from hospital websites included not just sensitive health information, such as details about medications, allergies, and upcoming doctor visits, but also

---

[19] *Private Health Data Still Being Exposed to Big Tech, Report Says*, INSURANCE JOURNAL (Oct. 17, 2023), https://www.insurancejournal.com/news/national/2023/10/17/744625.htm [https://perma.cc/M8YP-WDKU].

[20] Timothy Libert, *Privacy Implications of Health Information Seeking on the Web*, COMMUNICATIONS OF THE ACM (March 2015), http://timlibert.me/pdf/Libert-2015-Health_Privacy_on_Web.pdf [https://perma.cc/NC4F-5GRZ].

[21] *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP, https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites [https://perma.cc/3X7W-MMJB].

personally identifiable information, including patients' names, addresses, email addresses, and phone numbers.

115. Additionally, The Markup's investigation found that the Meta Pixel was embedded in public-facing hospital websites and within password-protected patient portals at seven health systems, including FastMed and Novant Health.[22]

116. The FTC has taken enforcement action against Internet providers who track sensitive health data.

117. For example, in June 2022, the FTC finalized a settlement with Facebook regarding its covert collection of sensitive medical data when Flo, an ovulation tracking app, shared users' private health information with Facebook[23] and other advertisers.[24]

III. The Unauthorized Collection of Personal Health Data Contravenes Legal, Ethical, and Social Norms

A. Website Users Reasonably Expect Personal Health Information to Be Confidential.

---

[22] *Id.*

[23] *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*, FTC (Jun 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google [https://perma.cc/V33W-LEEE].

[24] Justin Sherman, *Your Health Data Might Be for Sale*, SLATE (Jun 22, 2022, 5:50 AM), https://slate.com/technology/2022/06/health-data-brokers-privacy.html [https://perma.cc/L7U4-4VMW].

118. Personal health data collected by Tracking Pixels, Session Replay Code, and other tracking technologies may be "highly personal information that people choose not to disclose even to family, friends, or colleagues," which nevertheless "is actually shared with complete strangers."[25]

119. According to the FTC, personal health information is "[a]mong the most sensitive categories of data collected by connected devices[.]"[26]

120. Personal health information collected by websites "may pose an incalculable risk to personal privacy."[27] The practice of allowing Third-Party Vendors to "collect that data, combine it, and sell or monetize it" would be an "unprecedented intrusion."[28] That is exactly what Defendant has done, and is still doing.

---

[25] *Report: Companies Continue to Share Health Data Despite New Privacy Laws*, Consumer Reports (Jan. 16, 2024), https:advocacy.consumerreports.org/wp-content/uploads/2024/01/Companies-Continue-to-Share-Health-Data-1-16-2024-Consumer-Reports.pdf [https://perma.cc/7WFB-BBTW].
[26] Kristin Cohen, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, FTC (July 11, 2022) https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal [https://perma.cc/67CF-PZ3Y].
[27] *Id.*
[28] *Id.*

121. Consumers' confidence that their personal and private health data will be kept secure is a major public health issue.

122. A 2015 review found that "the social stigma associated with some health conditions is among the top reasons consumers delay or avoid getting help for mental health problems."[29]

123. The fear of "disclosure and confidentiality concerns" was a prominent cause of this stigma.[30]

124. Once a person's private and sensitive health information is available, it exposes that individual to significant harm.

125. Criminals and other malevolent actors use personal health data to facilitate phishing scams, commit identity theft, and inflict physical or emotional injury.[31]

126. Information about private health and medical matters, including data related to sexual activity or reproductive health, "may

---

[29] *Report: Companies continue to share health data despite new privacy laws*, CONSUMER REPORTS (Jan. 15, 2024), https://advocacy.consumerreports.org/research/report-companies-to-share-health-data-despite-new-privacy-laws/ [https://perma.cc/2WRY-6QAB].

[30] *Id.*

[31] Kristin Cohen, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, FTC (July 11, 2022) https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal [https://perma.cc/67CF-PZ3Y].

subject people to discrimination, stigma, mental anguish, or other serious harms."[32]

B. Private Heath Information Can Be Harvested for Commercial Gain.

127. Companies that collect private information "have a profit motive to share data at an unprecedented scale and granularity."[33]

128. Once an individual's personal and private health data are collected, they "often have no idea who has it or what's being done with it."

129. The data "enters a vast and intricate sales floor frequented by numerous buyers, sellers, and sharers."[34]

130. In a 2014 study, the FTC reported that data brokers use data collected from consumers to create profiles that may contain sensitive inferences, such as categorizing someone as an "expectant parent."[35]

---

[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*; *Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission*, FTC (May 2014), https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014 [https://perma.cc/4LSS-RTV6].

131. Once these invasive and sensitive profiles have been created, the brokers use them to target "personalized" ads.[36]

132. The categories that consumers are placed into can be incredibly private or invasive, such as "working-class mom," "frequent alcohol drinker," "financially challenged," or "depression sufferer."[37]

133. In the same 2014 study, one data broker, Acxiom, bragged to shareholders that it had 3,000 points of data for nearly every consumer in the United States.[38]

134. Data aggregators and brokers gather this collected personal data and "sell access to it (or analyses derived from it) to marketers, researchers, and even government agencies."[39]

135. The scale of the personal and private data flowing from users to brokers is staggering.

---

[36] *Id.*
[37] *Online Advertising & Tracking,* EPIC, https://epic.org/issues/consumer-privacy/online-advertising-and-tracking/. [https://perma.cc/8CGL-4AQU].
[38] *Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission*, FTC (May 2014), https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014 [https://perma.cc/4LSS-RTV6]; Kristin Cohen, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, FTC (July 11, 2022) https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal [https://perma.cc/67CF-PZ3Y].
[39] *Id.*

136. The sheer number of ads shown to Internet users is overwhelming, with Americans exposed to an estimated 5,000 ads daily.[40]

137. According to the FTC, "some popular ad exchanges can handle tens of billions of auctions per day. Each auction involves a broadcast of consumer data being sent to potentially dozens of bidders simultaneously, despite only one of those parties – the winning bidder – actually using that data to serve a targeted ad."[41]

138. Once private and personal data are in the hands of data brokers, "there are few (if any) technical controls ensuring that [they] do not retain that data for use in unintended ways."[42]

C. Regulatory Authorities Prohibit the Unauthorized Collection and Tracking of Private Health Information.

139. Defendant, as a health insurance issuer and a provider of health plans (including employer-sponsored group health plans), is a "covered entity" under HIPAA.

---

[40] *Id.*
[41] *Unpacking Real Time Bidding through FTC's case on Mobilewalla*, FTC (Dec. 3, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla [https://perma.cc/8WYU-UPGW].
[42] *Id.*

140. The U.S. Department of Health and Human Services ("HHS") has issued a bulletin covering the use of online tracking technologies, such as Tracking Pixels and Session Replay Code, by these HIPAA-covered entities. The bulletin clarifies the privacy and security rules promulgated under HIPAA, 42 U.S.C. §§ 1320d–1320d-9.

141. The HHS bulletin states that "[r]egulated entities are not enabled to use tracking technology in a manner that would result in impermissible disclosures of [PHI] to tracking technology vendors or any other violations of the HIPAA rules."[43]

142. The bulletin continues, "[f]or example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures."[44]

143. The bulletin further explains that the PHI collected by tracking technologies placed on websites, such as Tracking Pixels and Session Replay Code, can include "an individual's medical record

[43] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html. [https://perma.cc/LT73-TWQD].
[44] *Id.*

number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, device IDs, or any unique identifying code."[45]

144. Defendant's use of tracking technologies on the Website, such as Tracking Pixels, violates the HHS bulletin, which explicitly states that regulated entities like Defendant are not permitted to use tracking technologies in a manner that leads to impermissible disclosures of PHI to third parties without obtaining HIPAA-compliant authorizations.

145. The HHS bulletin further clarifies that disclosure of PHI to vendors for marketing purposes (including targeted advertising or analytics used to improve advertising performance) violates HIPAA without HIPAA-compliant authorization from the individual.

146. Defendant's conduct, including enabling Third-Party Vendors to track insureds on Defendant's Website for advertising purposes, is exactly the type of unauthorized data sharing of sensitive medical information that the HHS bulletin states is prohibited.

[45] *Id.*

147. On user-authenticated websites, which require a user to log in before gaining access to the site, tracking technologies may "have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal."[46]

148. Even on unauthenticated websites, which do not require users to log in before gaining access to the website, tracking technologies may obtain access to an individual's PHI.

149. The HHS bulletin gives the following example: "[I]f an individual were looking at a hospital's webpage listing its oncology services to seek a second opinion on treatment options for their brain tumor, the collection and transmission of the individual's IP address, geographic location, or other identifying information showing their visit to that webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual's health or future health care."[47]

[46] *Id.*
[47] *Id.*

150. The HHS bulletin outlines the harms that disclosure of PHI may cause, including "identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI."[48]

151. The disclosure of an individual's PHI "can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment."[49]

152. In a joint letter sent on July 23, 2023, to hospital systems and telehealth providers, the FTC and the HHS Office for Civil Rights also reiterated the risks posed by the disclosure of an individual's personal health information to third parties.

153. The joint letter noted that such disclosures could reveal "sensitive information including health conditions, diagnoses,

[48] *Id.*
[49] *Id.*

medications, medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment."[50]

154. At the state level, Michigan grants protections for medical records, including MCL 333.20175 ("A health facility or agency shall maintain the records required under subsection (1) in such a manner as to protect their integrity, to ensure their confidentiality and proper use, and to ensure their accessibility and availability to each patient or the patient's authorized representative as required by law"); MCL 550.1406 ("A health care corporation shall, in order to ensure the confidentiality of records containing personal data that may be associated with identifiable members, use reasonable care to secure these records from unauthorized access and to collect only personal data that are necessary for the proper review and payment of claims and for health care operations, treatment, and research."); and MCL 333.26261–333.26271 (governing access to and disclosure of medical records).

[50] *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, FTC (July 20, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking [https://perma.cc/EB3S-UF3V].

155. The American Medical Association's ("AMA") *Code of Medical Ethics* also promulgates rules that protect the privacy of patient data and communications, which apply to Defendant.

156. These AMA rules include, but are not limited to, *AMA Code of Medical Ethics* Opinion 3.1.1 ("[p]atient privacy encompasses a number of aspects, including . . . personal data"); Opinion 3.2.4 ("Information gathered and recorded in association with the care of the patient is confidential."); and Opinion 3.3.2 ("Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored.").

IV. Confidentiality Expectations in Member Portals

157. Password-protected portals are subpages of a health insurer's website to which insureds gain access only after registering, verifying identity, and logging in with credentials.

158. These portals typically provide individualized services to insureds, including the ability to research medical and health issues, view insurance claims, obtain explanations of benefits, track insurance

deductibles, review prescriptions, and update member profile information.[51]

159. Portals function as live dashboards, providing, among other things, updates on claims, prescriptions, lab results, and secure messaging. Because these updates are continuous, portal activity creates a detailed summary of an individual's health. Studies show that increased portal use is associated with better health outcomes.[52]

160. Portal content is nonpublic and tailored to each insured; it is not accessible to anonymous website visitors.

161. Because portal interactions are tied to a specific insured's identity, the data displayed or transmitted often constitutes IIHI, a category of PHI under HIPAA. 45 C.F.R. § 160.103.

162. From an insured's perspective, logging into a portal signals entry into a private communication channel with the insurer in which

[51] Courtney R. Lyles, Janey Hamblin, Victor Y.X. Lin, Dean Schillinger, *Legal, Practical, and Ethical Considerations for Making Online Patient Portals Accessible for All*, 107 AM. J. PUB. HEALTH 1608 (2017), https://pmc.ncbi.nlm.nih.gov/articles/PMC5607665/pdf/AJPH.2017.303933.pdf [https://perma.cc/U52A-RE2Q].
[52] *Id.*

there is an expectation that health information shared in the portal will be kept confidential.[53]

V. Defendant Covertly Intercepted Plaintiffs' Sensitive Private Health Information for Commercial Profit

A. Defendant Covertly Wiretaps Website Communications Within Its Public-Facing Website and Portals.

163. Despite deep public concerns about Internet privacy and the sensitivity of personal health-related data, Defendant unlawfully embedded code on its public-facing Website that allows Third-Party Vendors to harvest, for financial benefit, the sensitive private health information of Defendant's insureds.

164. Defendant further benefits from Tracking Technologies on the public-facing pages of the Website, as such data allows the Defendant to identify groups or segments among its insureds and refine marketing to increase enrollment and revenue.

165. Defendant operates one primary patient portal ("Main Portal") at the web address of member.bcbsm.com. After insureds enter their login credentials, they can review medical treatment options,

[53] *K.L. v. Legacy Health*, No. 23-1886, 2024 U.S. Dist. LEXIS 206864, at *9 (D. Or. Nov. 14, 2024).

retrieve information regarding their medical benefits, and access summaries of their health visits, among other actions involving highly sensitive medical and financial data.

166. Insureds seeking to locate a pharmacy or update their prescriptions are directed within the primary portal to bcbsm.benefitrx.com ("Prescription Portal") within which they can engage with Optum Rx, a pharmaceutical company that serves as the pharmacy benefit manager for Defendant.[54]

167. Insureds are not prompted to re-enter their login credentials upon transfer to the Prescription Portal, nor do they receive notice that they are being redirected.

168. Insureds seeking behavioral health and wellness resources are redirected to the web address of www.liveandworkwell.com ("Wellness Portal"), one of Optum Rx's "private support tools."[55]

169. Within the Wellness Portal, insureds search for providers or programs targeted at specific behavioral conditions and ailments.

---

[54] *Welcome to Optum Rx*, OPTUM, INC., https://www.optumrx.com/ [https://perma.cc/XJ5Q-P9PS].

[55] *About Us*, OPTUM LIVE AND WORK WELL, https://www.liveandworkwell.com/en/public/help/about-us [https://perma.cc/U6U9-QKJB].

170. As with the Prescription Portal, insureds are not prompted to re-enter their login credentials upon transfer to the Wellness Portal, nor do they receive notice that they are being redirected.

171. Defendant has surreptitiously embedded the Tracking Technologies of the Third-Party Vendors within the public-facing pages of the Website, Main Portal, Prescription Portal, and Wellness Portal.

B. Defendant Enables Verint's Tracking Technologies on Defendant's Purportedly "Secure" Patient Portals.

1. Verint as a Tracking Vendor

172. Defendant has embedded the Tracking Technologies of Third-Party Vendor Verint within the secure patient portals of the Website, enabling the interception and collection of insureds' private data and communications, including health-related queries, without insureds' consent.

173. Verint is a provider of customer experience analytics, headquartered in Melville, New York, which markets and deploys an analytics platform that collects a wide range of insureds' data on behalf of its clients.[56]

[56] *Predictive Modeling*, VERINT SYS., INC., https://www.verint.com/voice-of-the-customer/predictive-modeling/ [https://perma.cc/3L2W-72LR].

174. Verint's Interaction Analytics tool purports to enable customers to "interact with [their] customers on whatever channel they choose while uncovering valuable insights – regardless of where or how these interactions take place."[57]

175. Furthermore, its Knowledge Management system gathers information to predict which "Help" articles an insured is likely to be interested in: the Knowledge Management system "[u]ses information about customers, such as their location, products owned, and active cases to drive what knowledge articles are likely to be needed."[58]

176. Verint enables real-time tracking of insureds' interactions across the Website, including personally identifiable information like name, email address, or phone number.

177. Tracked interactions can also include sensitive personal health information, such as insureds' queries of terms associated with medical ailments.

---

[57] *Interaction Analytics*, VERINT SYS. INC., https://www.verint.com/interaction-analytics/ [https://perma.cc/DAV5-987S].
[58] *The Complete Guide to Knowledge Management*, VERINT SYS. INC., https://www.verint.com/knowledge-management-guide/ [https://perma.cc/K7RA-R2P4].

2. Tracking on Portal Entry, Subpages, and Unique Identifiers

178. Network traffic inside the Website patient portals is directed to computers operated and controlled by Verint.

179. When an insured reaches the Website's patient portal landing page on the Main Portal, a Verint request with embedded JavaScript code serving directly to Verint's analytics engine loads simultaneously, *before* the insured takes any actions:

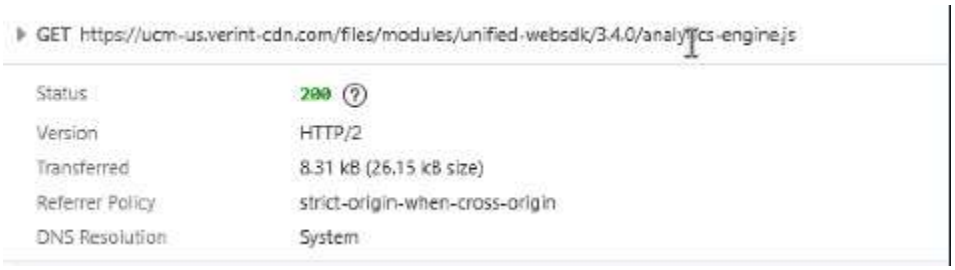


Figure 2

180. Similarly, when an insured checks the status of their prescriptions on the "Prescriptions" subpage and Prescription Portal, a request from Verint with embedded JavaScript code simultaneously loads:

Figure 3

181. An identical URL makes a request in the Main Portal when an insured selects the "Specialty Care" designation of the "Find Care" tool and searches for care based on a sensitive medical condition, like typing "back pain," into the search field when prompted:

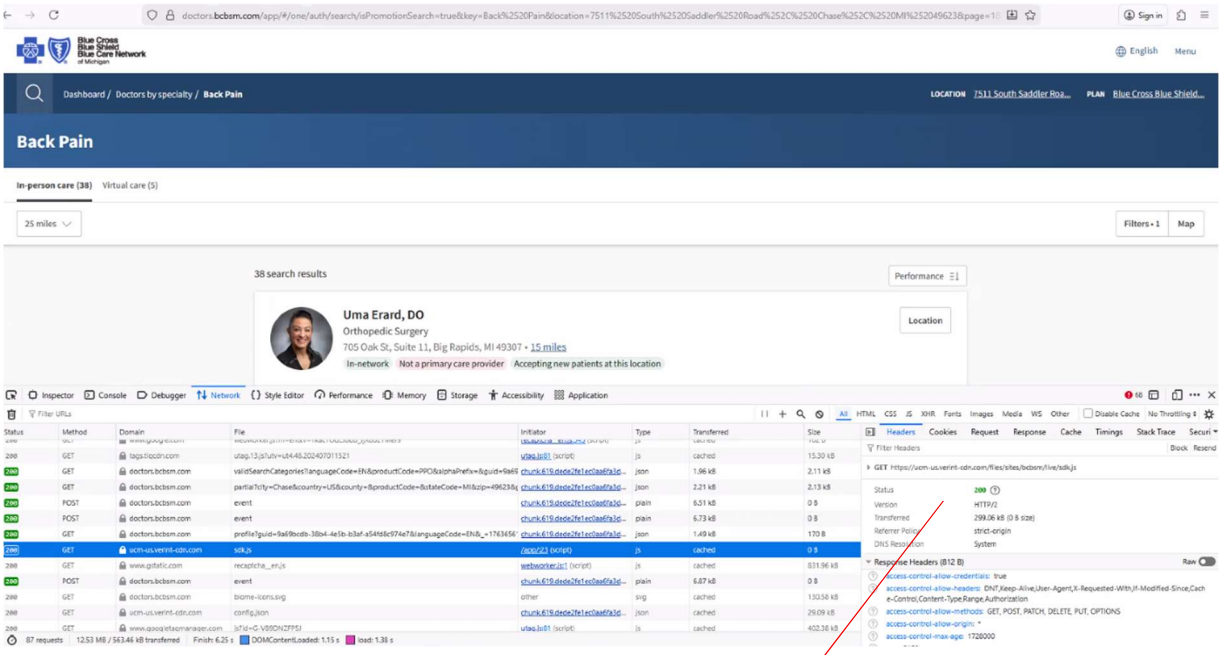


Figure 4

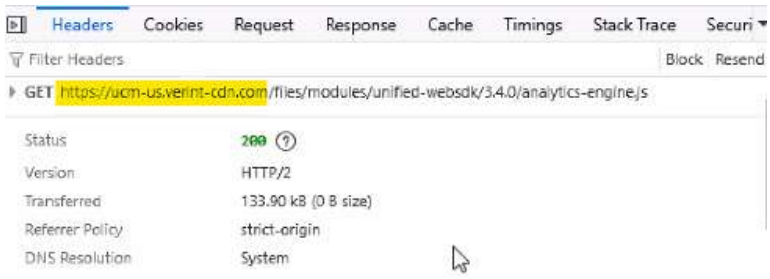


Figure 5

182. Verint does not collect this data in the aggregate; it pins it to specific insureds and collects specific insureds' private data. Figure 5, above, shows how information associated with insureds' interactions within Website patient portals (such as review of information related to medical ailments) are captured, catalogued, and transmitted to Verint computers.

C. Defendant Enables Adobe's Tracking Technologies on Defendant's Purportedly "Secure" Patient Portals.

1. Adobe as a Tracking Vendor

183. Adobe is another Third-Party Vendor for which Defendant has embedded Tracking Technologies, which enable Adobe to harvest the private data of users of Defendant's secure patient portals for marketing and commercial purposes, without clearly disclosing Adobe's role on the Website to insureds or obtaining consent.

184. Adobe is a software company headquartered in San Jose, California. While known for its products like Photoshop and Acrobat, it also operates a number of digital marketing and data analytics tools used to track behavior across websites.

185. These data products include Adobe Analytics,[59] Adobe Experience Manager,[60] and Adobe Audience Manager,[61] all of which use Tracking Technologies like beacons, pixels, JavaScript tags, cookies, and Session Replay Code to capture data in real time.

186. Defendant embedded Adobe's Tracking Technologies on the Website.

187. Defendant's embedding of Adobe's Tracking Technologies on the Website allowed Adobe to surreptitiously harvest data about insureds' visits, including keyword searches, and potentially match that data to offline profiles.

2. Adobe Tracking on Portal Entry and Main Portal

188. When an insured reaches the landing page of the Main Portal, Adobe executes a request for their data even *before* the insured takes action on the page:

---

[59] *Adobe Analytics*, ADOBE FOR BUSINESS, https://business.adobe.com/products/adobe-analytics.html [https://perma.cc/MX45-HTSE].
[60] *Adobe Experience Manager*, ADOBE FOR BUSINESS, https://business.adobe.com/products/experience-manager/sites/aem-sites.html [https://perma.cc/3X55-WWKT].
[61] *Adobe Audience Manager*, ADOBE FOR BUSINESS, https://business.adobe.com/products/audience-manager/adobe-audience-manager.html [https://perma.cc/C5DG-89MH].

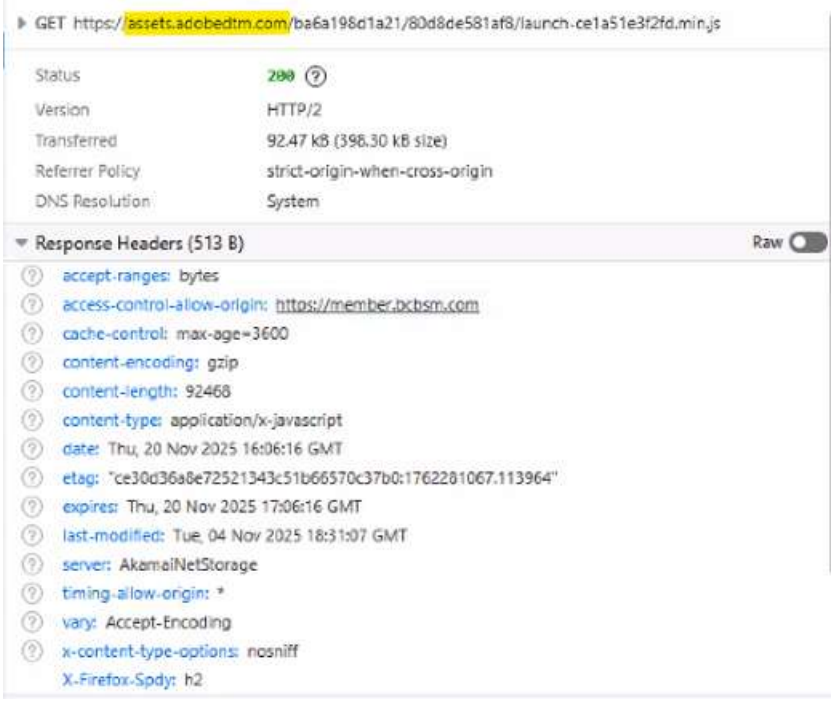


Figure 6

189. As shown in the above Figure 6, Defendant's Website loads third-party tracking code from Adobe via a request to https://assets.adobedtm.com, a domain controlled by Adobe's Digital Tag Manager ("DTM").

190. DTM is a platform designed to insert JavaScript code, such as the above, into websites like Defendant's Website, enabling Adobe to "collect data from [a] website's visitors so [they] can analyze that data

and use it to carry out tasks such as product recommendations, live chat, and advertising."[62]

191. Adobe also carries out requests via the domain smetrics.bcbsm.com, which represents Adobe's analytics collection server.

192. For example, the following request loads when the insured reaches the Main Portal's landing page:

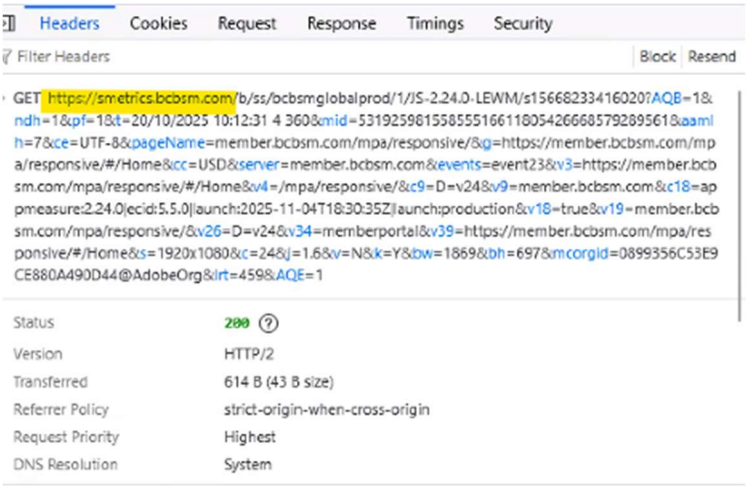


Figure 7

[62] *Tag management – what it is and how it works*, ADOBE FOR BUSINESS, https://business.adobe.com/blog/basics/tag-manager [https://perma.cc/CM72-2JHS].

193. The above request also contains multiple embedded persistent identifiers intended to begin building a user profile even *before* the insured takes action inside the portal.

Figure 8

194. As seen in Figure 8, above, Adobe assigns the insured an identifier beginning with "0899…" via an Adobe Experience Cloud-operated AMCV cookie.[63] Additionally, the insured's network traffic is directly linked to their patient portal user name via an additional embedded cookie (*see* "User_Name" in Figure 8) (redacted in this Complaint to preserve client confidentiality).

195. Adobe further identifies the insured through a unique string of characters beginning "403…" associated with a cookie titled

[63] *Cookies and the Experience Cloud Identity Service*, ADOBE EXPERIENCE LEAGUE, https://experienceleague.adobe.com/en/docs/id-service/using/intro/cookies [https://perma.cc/GEU5-MFQH].

"PERSON_ID," as well as through the collection of an IP address (*see* Figure 8, above, "SOB_IP_Address").

196. This setup enables Adobe to receive the full content of Website Communications between insureds and Defendant's Website on the Main Portal. That includes sensitive health-related search queries, button clicks, and navigation activity that reveal the insureds' medical interests, insurance status, or treatments.

3. Adobe Tracks Insureds' Research in Wellness Portal

197. Adobe also tracks insureds' research within the Wellness Portal. For example, when an insured interacts with an article titled "Everything You Need to Know About ADHD" on a Wellness Portal subpage titled "Mental Health", Adobe transmits not only the *full and exact* name of the condition referenced in the article, but also multiple persistent identifiers.

198. Below is a portion of the data payload (i.e., the data related to what the insured clicked or typed) associated with this request with relevant highlights:[64]

[64] This payload is associated with a request executed after an insured clicked on an article titled "Everything You Need to Know About ADHD" as they navigated through the "Mental Health" subpage of the Wellness Portal

AQB=1&ndh=1&pf=1&t=20%2F10%2F2025%2011%3A34%3A19%204%20360&cid.&uuid_hsid.&id=b28069d7-ea80-49ba-b29b-962d5a831c28&as=1&.uuid_hsid&UUID.&id=b28069d7-ea80-49ba-b29b-962d5a831c28&as=1&.UUID&.cid&sdid=14684AF898B12794-2A0817D25AB74CD0&mid=69347446520983626153840658990365239596&aamlh=7&ce=UTF8&ns=unitedhealthgroup&pageName=optum%3Alaww%3Aarticle%20page&g=https%3A%2F%2Fbh.liveandworkwell.com%2Fcontent%2Fen%2Fmember%2Farticle.16252.html&r=https%3A%2F%2Fbh.liveandworkwell.com%2Fen%2Fmember%2Fmind-body%2Fmental-health%2Fadhd.html&c.&p_fo=3.0&getPageLoadTime=2.0.2&performanceWriteFull=1.0&performanceWritePart=1.0&performanceCheck=1.0&getNewRepeat=3.0.1&apl=4.0&.c&cc=USD&aamb=RKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y&c1=2.5.0%7Eproduction%7E2025-02-03T12%3A34%3A52Z%7ELive%20And%20Work%20Well%20%28DTM%20-%202019-10-17%2006%3A04%3A34%29&v1=optum&h1=optum%3Alaww%3A&c2=2.5.0%3A2025-02-03t12%3A34%3A52z&v2=laww&v3=https%3A%2F%2Fbh.liveandworkwell.com%2Fcontent%2Fen%2Fmember%2Farticle.16252.html&c6=D%3Dv5&c8=D%3Dv8&c14=D%3Dv14&v14=optum%20digital&c16=optum%3Alaww%3Aarticle%20page&v16=optum%3Alaww%3Aarticle%20page&c17=D%3Dv17&c22=D%3Dv22&v22=consumer&c23=D%3Dv23&v23=loggedin&c24=new&v24=new&c25=D%3Dv25&v25=optum%3Alaww%3Aarticle%20page&c26=D%3Dv26&v26=9%7C9&c33=D%3Dv33&c34=D%3Dv34&v34=11054&c35=D%3Dv35&c36=D%3Dv36&c37=D%3Dv37&v37=laww%3Aproducts%2Fcoreproducts%2Fbh&c38=D%3Dv38&v38=everything%20you%20need%20to%20know%20about%20adhd&c39=D%3Dv39&v39=_6_private&c41=D%3Dv41&c44=Page%20Load%20Rule%20

199. The payload shows how Adobe learned which medical topic interested the insured in the Wellness Portal. The request reports the page's subject matter (i.e., "ADHD," or Attention-Deficit/Hyperactivity

Disorder), along with the insured's logged-in status and other identifiers.

200. For example, Adobe advertises its use of the "mid" cookie to "set and store a unique ID for [customers'] site visitors" and "track users across [customers'] domains."[65]

201. This payload allows Third-Party Vendors like Adobe to link sensitive medical information about a medical condition to an individual for marketing or profiling.

202. Similarly, when an insured visits the "Programs" subpage of the Wellness Portal, manually enters "depression" into the search field, and subsequently selects a page detailing postpartum depression, Adobe makes a request containing the full and exact search term, as well as the page title:[66]

> AQB=1&ndh=1&pf=1&t=20%2F10%2F2025%2011%3A27%3A37%204%20360&cid.&uuid_hsid.&id=b28069d7-ea80-49ba-b29b-962d5a831c28&as=1&.uuid_hsid&UUID.&id=b28069d7-ea80-49ba-b29b-962d5a831c28&as=1&.UUID&.cid&sdid=09074012F958457B-1BC6230321E5B99B&mid=69347446520983626153840658990365

[65] *Cookies and the Experience Cloud Identity Service*, ADOBE EXPERIENCE LEAGUE, https://experienceleague.adobe.com/en/docs/id-service/using/intro/cookies [https://perma.cc/GEU5-MFQH].

[66] This payload is associated with a request executed after an insured manually entered "depression" into a search field on the "Programs" subpage of the Wellness Portal

239596&aamlh=7&ce=UTF8&ns=unitedhealthgroup&pageName=optum%3Alaww%3Adepression%3Apostpartum%20depression&g=https%3A%2F%2Fbh.liveandworkwell.com%2Fcontent%2Fen%2Fmember%2Fmind-body%2Fmental-health%2Fdepression%2Fpostpartum-depression.html&r=https%3A%2F%2Fbh.liveandworkwell.com%2Fen%2Fmember%2Fmind-body%2Fmentalhealth%2Fdepression.html&c.&getNewRepeat=3.0.1&p_fo=3.0&getPageLoadTime=2.0.2

203. Not only does the above payload demonstrate how Adobe collects tracking metrics recreating the insured's journey across portal subpages, including any actions taken along the way, but also how it assigns the insured a universally unique identifier persistently associated with these metrics and search terms, thereby allowing Adobe and Third-Party Vendors to tailor marketing to the insured's condition.

4. Financial Tracking and Prescription Portal Tracking

204. Moreover, the same strings of characters used to identify the insured in Figure 8, above, appear in an Adobe request executed when the insured visits the "Claims" page of the Main Portal to engage with

sensitive information associated with the medical care that the insured received:

Figure 9

205. As seen in the above Figure 9, not only does the identifier assigned to the insured's session persist, but also the Adobe-embedded cookie collects more personally identifiable information such as PERSON_ID, IP address, and even user name (redacted to preserve client confidentiality) when the insured begins to interact with portal subpages containing personal financial information.

206. Not only is Adobe active on the Main Portal, but it continues to make requests via a custom domain suited for Defendant's Prescription Portal.

207. For example, as seen in the screenshot below, when an insured engages with the "Find a Pharmacy" tool, which requires the

input of location data or the name of a prescription, the domain smetrics.optum.com makes a request referred by the Prescription Portal:

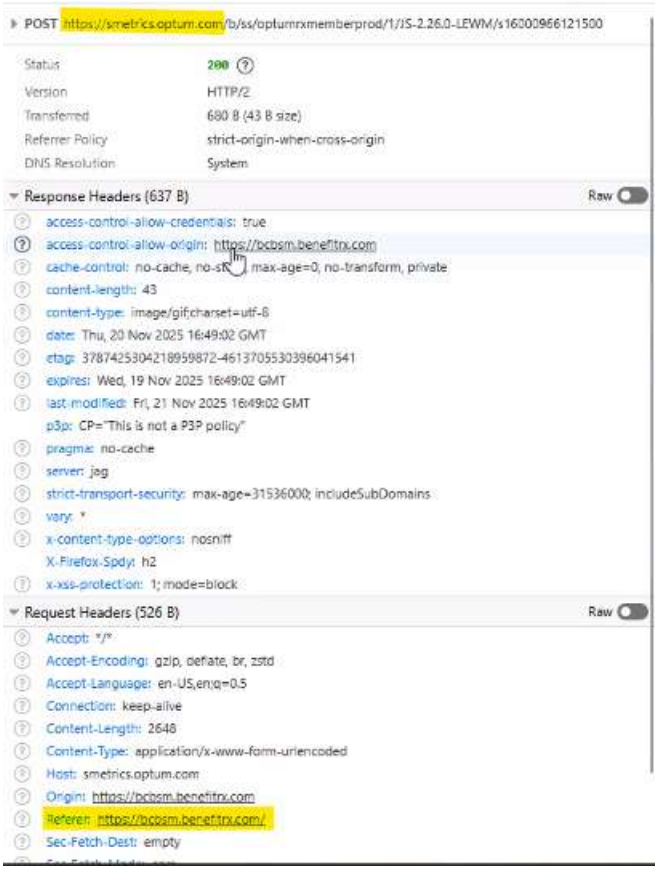


Figure 10

208. Additionally, when an insured clicks on a tile providing drug information for their prescription used to treat type 2 diabetes, Metformin, smetrics.optum.com sends a request with an embedded event titled "page track":

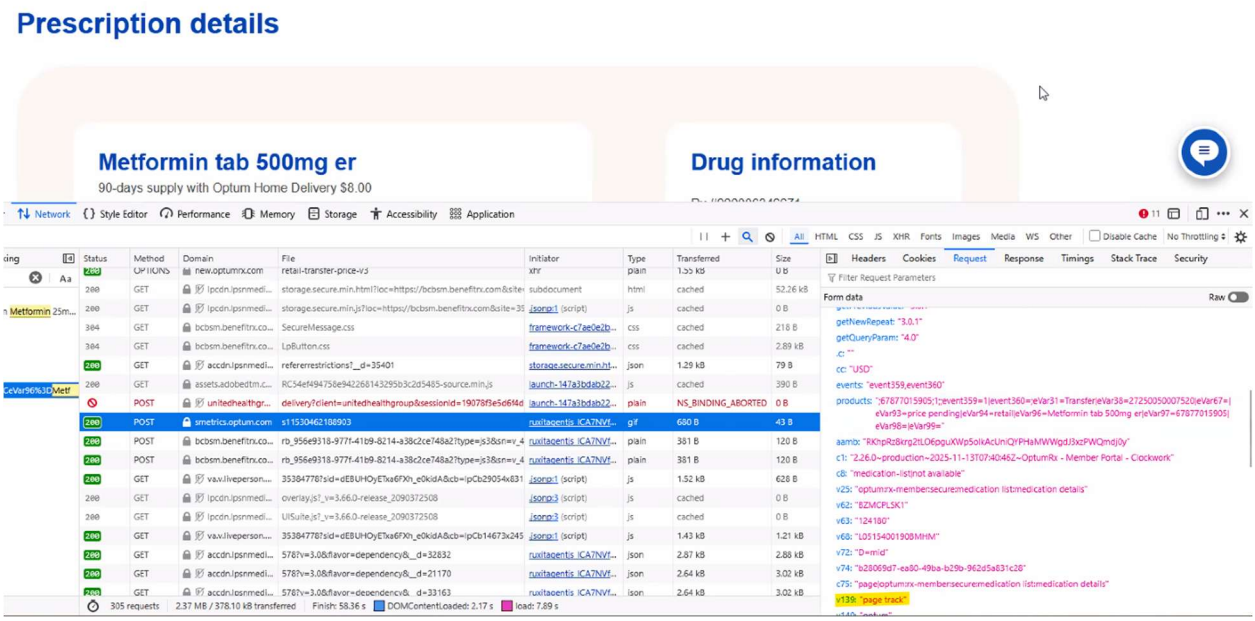


Figure 11

209. Adobe's tracking tools automatically send insureds' interactions in the Prescription Portal to Adobe's analytics systems.

5. Behavioral Health Tracking and Embedded Cookies

210. When an insured visits a subpage of the main portal titled "Behavioral and Mental Health" and subsequently selects "Crisis Care," Adobe gathers the name of the page, the time since the last visit to the

page, the date of the visit, and how long the session lasted, among other parameters:

Figure 12

211. Adobe collects similar metrics associated with the insured's session when the insured returns to the landing page of the Main Portal, this time with the *full and exact* name of the employer sponsoring the plan through which they are receiving medical benefits reflected in the request URL:

Figure 13

212. Adobe occasionally embeds cookies hosted by other Third-Party Vendors in its requests:

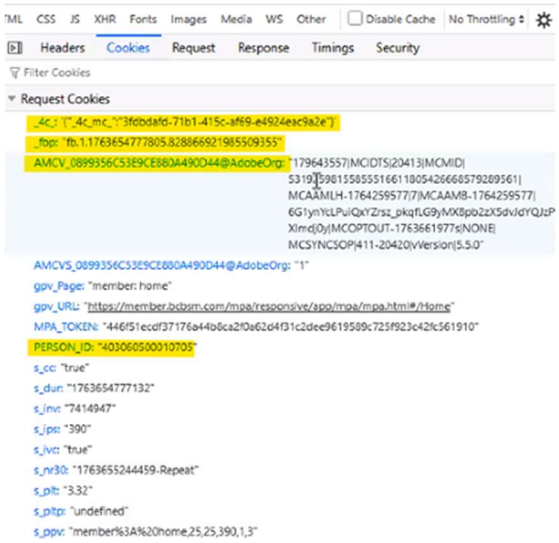


Figure 14

213. For instance, as shown in the above screenshot, taken when an insured visits the landing page of the Main Portal, Adobe embeds multiple persistent identifiers hosted by vendors such as ForeSee (acquired by Verint) (cookie beginning "_4c_") and Meta Pixel (cookie beginning "_fpb"). Adobe's AMCV produces an additional identifier, as well as the "Person_ID" cookie.

214. Similar smetrics.bcbsm.com requests are made when insureds reach the "Visit Summary" subpage of the Main Portal detailing the type and frequency of their medical visits (Figure 15), and even when they attempt to adjust their portal preferences (Figure 16):

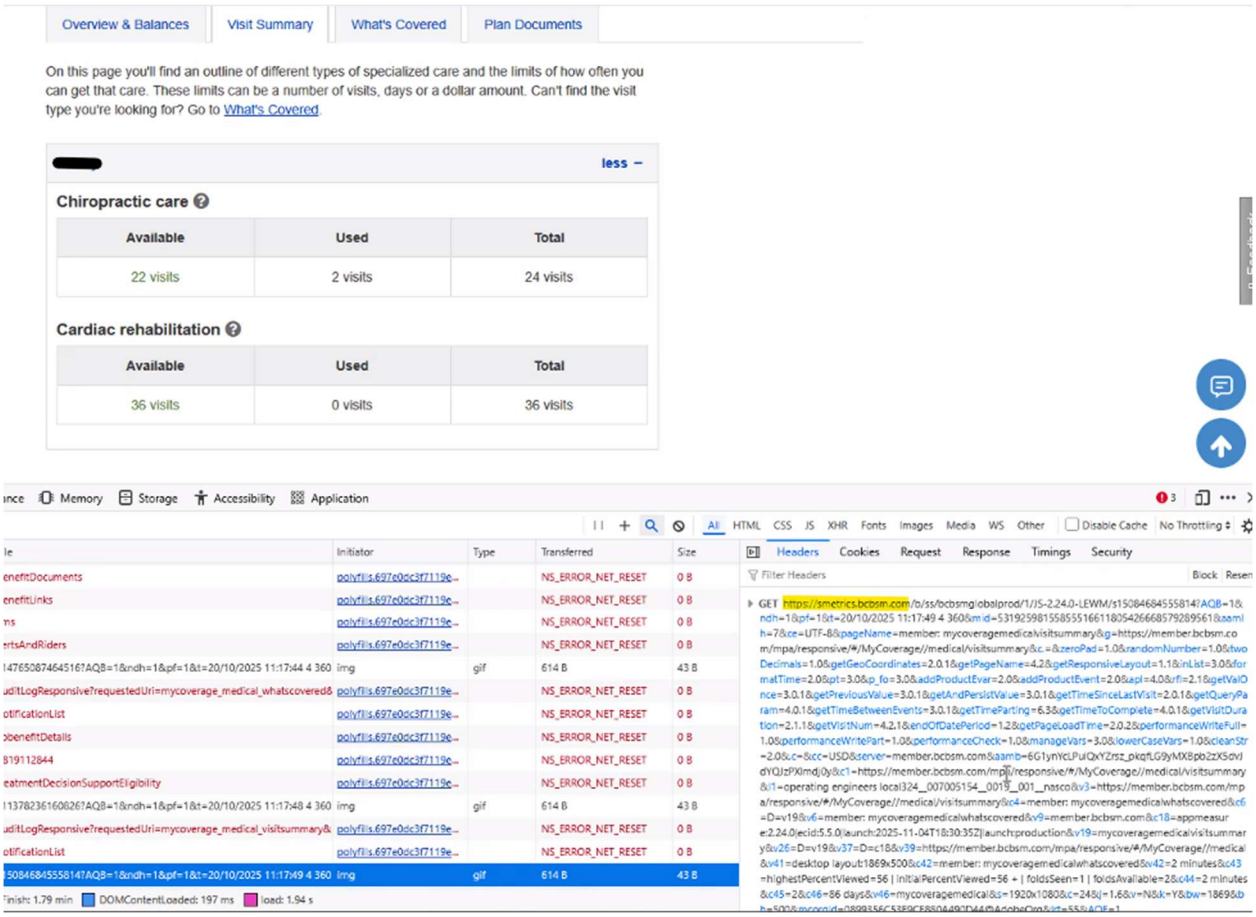


Figure 15

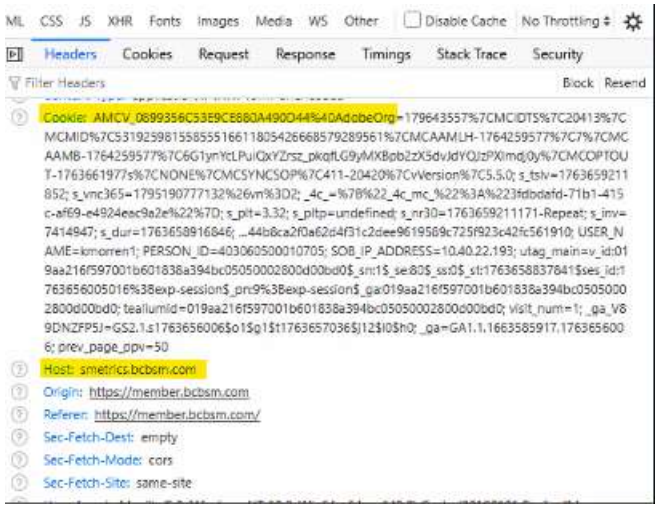


Figure 16

215. The smetrics is not an Adobe domain, but a subdomain of Defendant's own Website. Adobe's documentation[67] explains that smetrics.yourdomain.com is used so analytics traffic does not appear to originate from Adobe.

216. Adobe further admits that its configuration under smetrics is used to "bypass" browser tracking protections by tricking such protections into discerning that clients like BCBSM are the apparent source and controller of the data collection, not Adobe.[68]

217. Independent cybersecurity researchers describe this practice (known as CNAME cloaking) as a technique to disguise third-party tracking as first-party traffic and undermine user privacy protections.[69]

218. By routing Defendant's analytics through the BCBSM-branded subdomain for the express purpose of evading privacy safeguards, Defendant affirmatively chose to collect and transmit user data through infrastructure that it falsely presented as its own.

---

[67] *Privacy-first: Adobe Analytics cookie strategy*, ADOBE EXPERIENCE LEAGUE, https://experienceleague.adobe.com/en/perspectives/privacy-first-adobe-analytics-cookie-strategy [https://perma.cc/54ZH-L4Z7].
[68] *Id.*
[69] *CNAME Cloaking: Disguising Third Parties Through the DNS*, PALO ALTO NETOWRKS, https://unit42.paloaltonetworks.com/cname-cloaking/ [https://perma.cc/YL6M-UK74].

D. Defendant Enables Datadog's Tracking Technologies on Defendant's Purportedly "Secure" Patient Portals.

1. Datadog as a Tracking Vendor

219. Defendant has embedded the Tracking Technologies of Third-Party Vendor Datadog within the Website's secure patient portals enabling the interception and collection of insureds' private data and communications, including health-related queries, without insureds' consent.

220. Datadog is a software company based in New York, New York, which operates an observability and security platform for cloud applications.[70]

221. Datadog offers a real user monitoring ("RUM") platform that is adapted to both browsers and mobile applications, which captures detailed data about how users interact with websites.[71]

222. Datadog explicitly ties the RUM to potential revenue, boasting the tool's ability to "boost performance and understand user behavior" and assist entities like the Defendant to "[a]nalyze real user

[70] *Contact*, DATADOG, https://www.datadoghq.com/about/contact/ [https://perma.cc/3WGT-QTSS].
[71] *Real User Monitoring: Boost performance and understand user behavior*, DATADOG, https://www.datadoghq.com/product/real-user-monitoring/#improve-performance [https://perma.cc/LVE3-7VYK].

traffic and follow performance optimization flows to improve page performance."[72]

223. Datadog's tools collect information in "real-time" that easily allow identification of specific insureds, including IP address, browser and device type, and geographic location:[73]

The RUM Browser SDK generates events with associated metrics and attributes. Each RUM event contains all the default attributes , such as the page URL (`view.url`) and user information, such as their device type (`device.type`) and country (`geo.country`).

There are other metrics and attributes specific to a given event type . For example, metric `view.loading_time` is associated with view-type events, and attribute `resource.method` is associated with resource-type events.

EVENT TYPE	RETENTION	ROLE
Session	30 days	A user session begins when a user starts browsing the web application. A session includes general information about the user (browser, device, geolocation). It aggregates all RUM events collected during the user journey by applying a `session.id` unique attribute. **Note:** The session is reset after 15 minutes of inactivity.
View	30 days	A View event is generated each time a user views a page in the web application. As long as the user remains on the same page, Resource, Long Task, Error, and Action events are associated with this RUM view via the attribute `view.id` .
Resource	30 days	A Resource event is generated for images, XHR, Fetch, CSS, or JS libraries loaded on a web page. This contains detailed information about the loading time.
Long task	30 days	A Long Task event is generated whenever a browser task blocks the main thread for more than 50 ms.
Error	30 days	The RUM function collects all frontend errors thrown by the browser.
Action	30 days	RUM Action events record interactions made during each user journey and can also be sent manually to monitor custom user actions.

Figure 17

[72] *Id.*
[73] *RUM and Session Replay: RUM data collected (Browser)*, DATADOG, https://docs.datadoghq.com/fr/real_user_monitoring/browser/data_collected/ [https://perma.cc/CA4E-N7HL].

224. Like the other Third-Party Vendors, Datadog's Tracking Technologies are embedded throughout Defendant's Website, like in search bars where content is entered.

2. Datadog's Tracking of Portals' PHI

225. The following code from the prescription portal demonstrates how Datadog deploys its RUM technology, in this instance when an insured clicks through the "Find a Pharmacy" tool within the Prescription Portal:

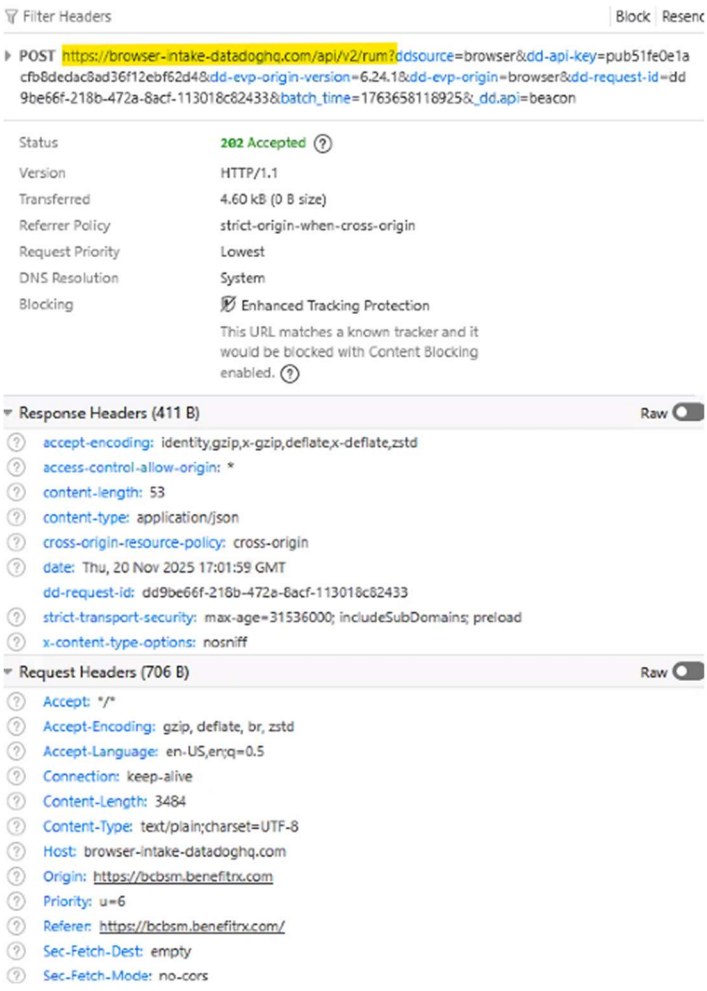


Figure 18

226. Figure 18, above, demonstrates how Datadog uses Tracking Technologies when insureds input sensitive information such as names of prescriptions.

227. A portion of the payload for this request reflects several Datadog commands such as "session_replay_sample_rate" and "profiling_sample_rate," and assigns the insured a unique identifier beginning with "4007":[74]

> {"type":"view","_dd":{"format_version":2,"drift":1,"configuration":{"session_sample_rate":100,"session_replay_sample_rate":0,"profiling_sample_rate":0,"beta_encode_cookie_options":false,"start_session_replay_recording_manually":true},"sdk_name":"rum","page_states":[{"state":"active","start":12460000000},{"state":"passive","start":36190000000}],"document_version":5},"application":{"id":"40074ca415484a8abdb0e6ac2490fdd4"},"date":1763657300476,"source":"browser","view":{"url":"https://bcbsm.benefitrx.com/secure/pharmacylocator?sso=BCBSMI%3Apharmacylocator%3Aprod%3A20210715%

228. Not only does Datadog intercept personal information that the insured inputs when searching for care, but it follows insureds as they navigate through Wellness Portal pages about specific, sensitive medical conditions:

[74] This payload is associated with a request executed when an insured selected the "Find a Pharmacy" tool in the Prescription Portal

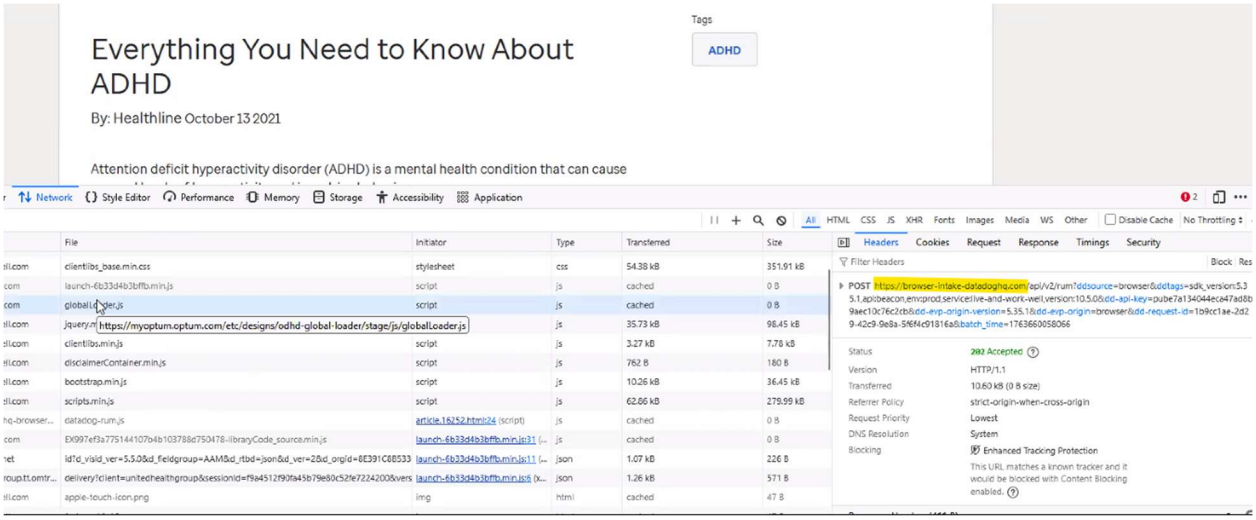


Figure 19

229. As seen in the above Figure 19, Datadog's RUM technology gathers and transmits metrics associated with the insured's session as they engage with an article titled "Everything You Need to Know About ADHD."

230. Datadog executes a similar request when the insured reaches the landing page of the Prescription Portal:

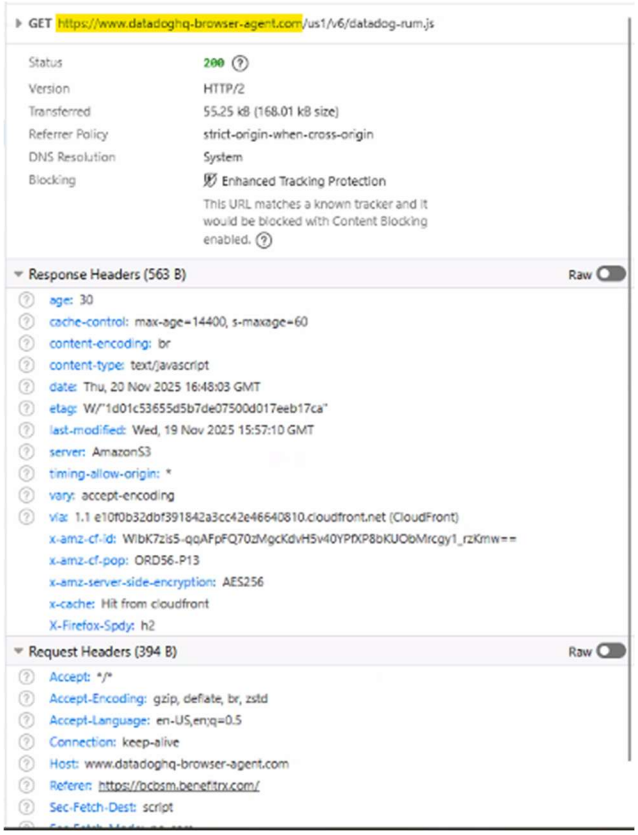


Figure 20

E. Defendant's Enabling of Qualtrics' Tracking Technologies on Defendant's Purportedly "Secure" Patient Portals.

1. Qualtrics as a Tracking Vendor

231. Defendant has embedded the Tracking Technologies of Third-Party Vendor Qualtrics within the secure patient portals to enable the interception and collection of insureds' private health-related data and Website Communications.

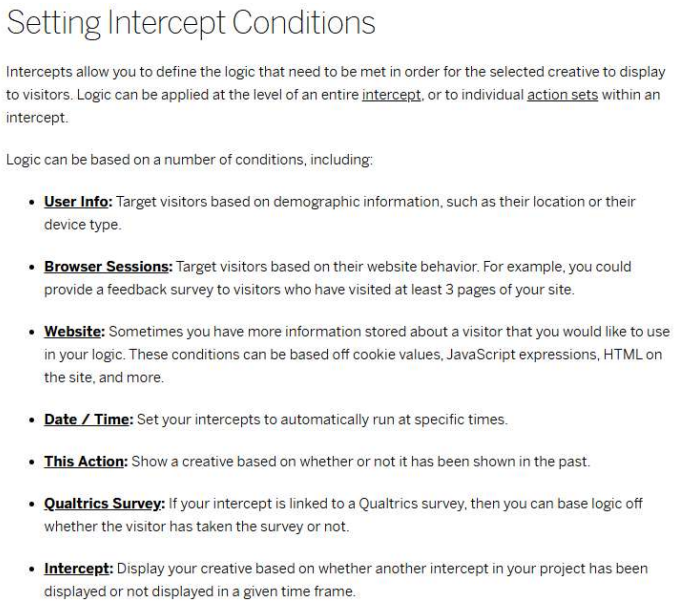
232. Qualtrics is a software company headquartered in Provo, Utah. Qualtrics' experience management platform operates a number of data analytics and session replay tools used to track user behavior across websites, enabling Qualtrics' customers like Defendant to "monitor every digital interaction, with behavioral breadcrumbs that turn your customers' movements into actionable insight."[75]

233. Qualtrics' tools purport to provide customers like Defendant the ability to "walk a mile in [their] customers' shoes" by "[w]atch[ing] replays of real-life customer sessions and track[ing] engagement across [their] website and mobile app […,] then make informed decisions that level up the customer experience."[76]

234. Furthermore, Qualtrics enables customers like Defendant to try out "intercepts" on their websites in order to help them decide where and how they should target content. Intercepts rely on certain session parameters gathered from a website:[77]

---

[75] *Digital Experience Analytics (DXA)*, QUALTRICS, https://www.qualtrics.com/customer-experience/digital-analytics/ [https://perma.cc/2BB2-EWV9].
[76] *Id.*
[77] *Setting Intercept Conditions*, QUALTRICS SUPPORT, https://www.qualtrics.com/support/website-app-feedback/getting-started-with-website-app-feedback/step-4-setting-up-your-intercept/ [https://perma.cc/Q8KN-Z6J3].



Setting Intercept Conditions

Intercepts allow you to define the logic that need to be met in order for the selected creative to display to visitors. Logic can be applied at the level of an entire intercept, or to individual action sets within an intercept.

Logic can be based on a number of conditions, including:

- **User Info:** Target visitors based on demographic information, such as their location or their device type.
- **Browser Sessions:** Target visitors based on their website behavior. For example, you could provide a feedback survey to visitors who have visited at least 3 pages of your site.
- **Website:** Sometimes you have more information stored about a visitor that you would like to use in your logic. These conditions can be based off cookie values, JavaScript expressions, HTML on the site, and more.
- **Date / Time:** Set your intercepts to automatically run at specific times.
- **This Action:** Show a creative based on whether or not it has been shown in the past.
- **Qualtrics Survey:** If your intercept is linked to a Qualtrics survey, then you can base logic off whether the visitor has taken the survey or not.
- **Intercept:** Display your creative based on whether another intercept in your project has been displayed or not displayed in a given time frame.

Figure 21

2. Qualtrics' Tracking Via Intercepts

235. Qualtrics' site interventions within Defendant's secure patient portals are often executed via the domain https://siteintercept.qualtrics.com. For instance, Qualtrics makes the following request when an insured visits the "Prescriptions" page of the Main Portal:

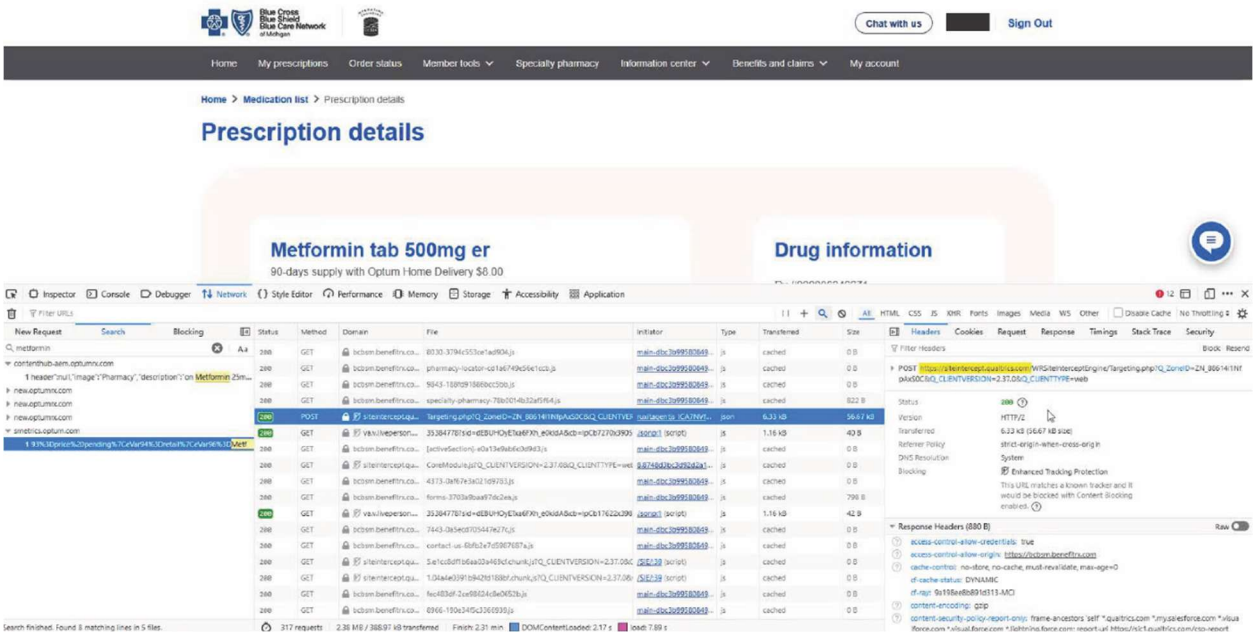


Figure 22

236. As seen in the above Figure 22, Qualtrics surreptitiously gathers data associated with the insured's session, including identifiers used to the track the session ("ZoneID"), the version of the tracking software ("CLIENTVERSION"), and the type of client environment ("CLIENTTYPE").

237. Not only is Qualtrics active in the Main Portal, but it is also active in the Prescription Portal:

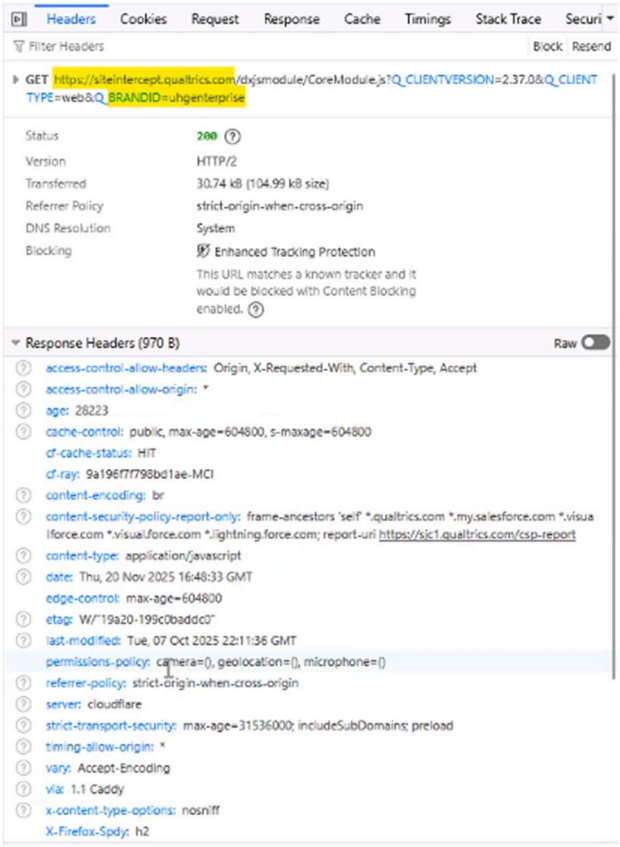


Figure 23

238. As seen in Figure 23, when an insured is browsing prescriptions, the browser initiates multiple requests to Qualtrics' servers. These requests also transmit data associating the insured's activity with their insurer through a brand identifier, "BRANDID."

239. Rather than occuring in a single transmission, Qualtrics deploys its Tracking Technologies via at least four distinct requests highlighted below in Figure 24 as the insured navigates the Prescription Portal:

Figure 24

240. As seen in the screenshot above, Qualtrics deploys several snippets of JavaScript code to carry out its data interceptions, the second of which appears to be associated with Datadog's RUM platform and contains a "targeting" tag.

241. The above code shows how Defendant has enabled Qualtrics to intercept insureds' data as they interact with Website subpages related to their prescriptions and benefits.

V. Plaintiffs Did Not Consent to Defendant's Interception, Harvesting, and Collection of Their Private Heath Data

A. Defendant Does Not Obtain Consent Prior to Surreptitiously Harvesting the Private Heath Data of Insureds.

242. Defendant's Website has an Online Privacy Practices section buried in its footer that represents how it "understands the importance of keeping your health information private":

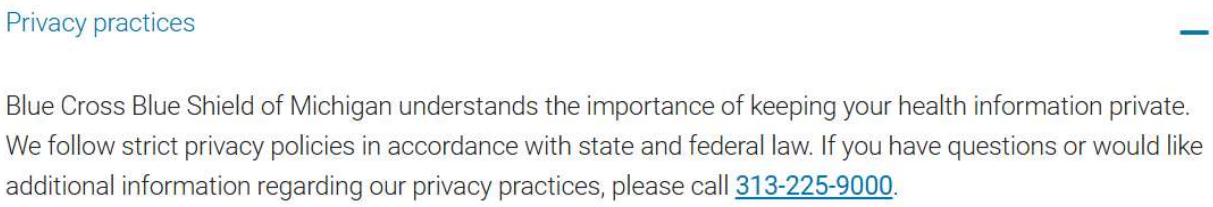


Figure 25[78]

243. In the same section of the Website, labeled Online Privacy Practices, Defendant further instructs insureds that if they believe their protected health information has been compromised, they should contact Defendant directly via telephone or email, and specifically cautions insureds not to include any protected health information in such communications:

[78] *Online Privacy Practices*, BCBSM, https://www.bcbsm.com/important-information/privacy-practices/ [https://perma.cc/G57X-QF66].

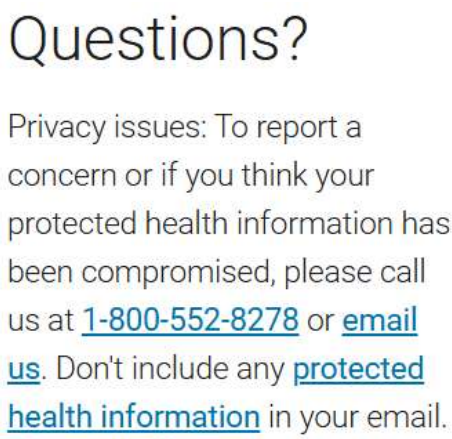


Figure 26[79]

244. This language conveys a professed commitment to the protection of insureds' data, particularly information, such as PHI, that is expressly subject to HIPAA and privacy laws and regulations.

245. On the same page, Defendant states that it makes a "pledge" to "consider any and all internet communications as private and confidential unless otherwise clearly stated":

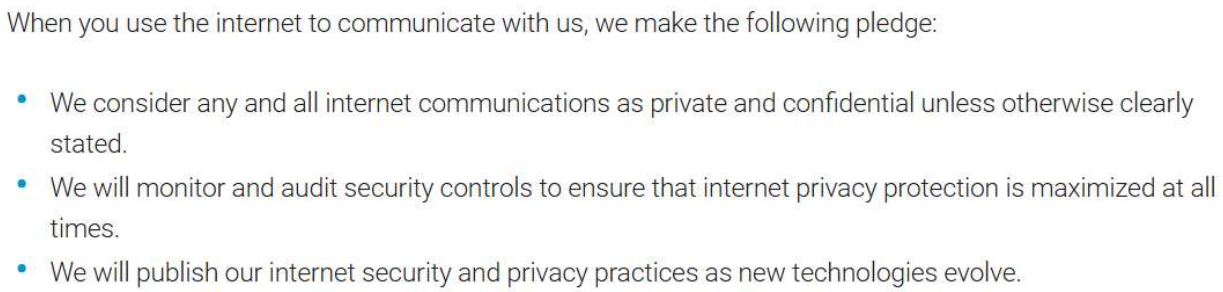


Figure 27[80]

[79] *Id.*
[80] *Id.*

246. These misrepresentations led insureds like Plaintiffs to reasonably believe that Defendant does not share or disclose sensitive health-related information or Website Communications to third parties without *express* authorization.

B. Unlawful Interception of Plaintiffs' Website Communications.

247. In reality, Tracking Technologies on Defendant's Website begin intercepting Website Communications *immediately* upon the loading of Defendant's Website.

248. Defendant's Website does not display a pop-up, banner, or consent prompt when insureds begin interacting with coverage tools, provider searches, or other health-related features.

249. Defendant's Website does not present its privacy policy in any conspicuous or easily accessible location before the tracking and data collection begins.

250. Instead, the privacy policy is buried in the footer of the homepage in a section misleadingly entitled "Online Privacy Practices," suggesting the practice of Defendant is to keep information private.

251. Plaintiffs were not informed that Tracking Technologies were being used on Defendant's Website, particularly not inside the secure portals.

252. When insureds navigate to Defendant's Website, they are not presented with any notification or alert regarding the sensitive health-related data collected by Tracking Technologies.

253. Such notifications, which may be referred to as "pop-up" or "clickwrap" agreements, require a website user to affirmatively consent to their data being collected, often by selecting an option stating "I agree," which Defendant's Website does not have.

254. In contrast to a conspicuous pop-up or notification, the privacy policy on Defendant's Website is in the bottom of a menu in the footer along with many other options:

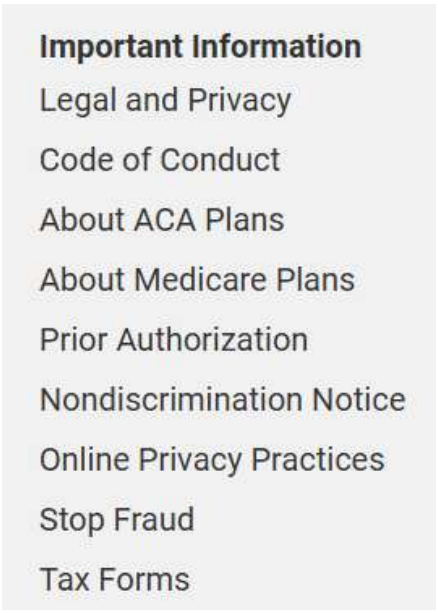


Figure 28[81]

255. Once an insured locates the "Online Privacy Practices"[82] link at the bottom of Defendant's Website and clicks on it, they are presented with several long text boxes that must be expanded to reveal content, such as "How we keep your PHI safe," "Accessing and sharing your own information," and "Protecting online interactions."

256. The second text box, titled "HIPAA," contains a hyperlink directing insureds to a seven-page PDF[83] that affirmatively states the insureds' written permission is required for use of their PHI (such as

[81] *Homepage*, BCBSM, https://www.bcbsm.com/ [https://perma.cc/WYV7-Q6YS].
[82] *Online Privacy Practices*, BCBSM, https://www.bcbsm.com/important-information/privacy-practices/, [https://perma.cc/VJK5-BNPE].
[83] *Notice of Privacy Practices*, BCBSM, https://www.bcbsm.com/amslibs/content/dam/public/common/documents/npp-nongroup-underwr-102612.pdf [https://perma.cc/A492-2W84].

their searches for "depression" or "back pain") and gives the false impression that Tracking Technologies are *not* being used:

- **For marketing communications:** Uses and disclosures of your PHI for marketing communications will not be made without a signed authorization except where permitted by law.
- **Sale of PHI:** We will not sell your PHI without a signed authorization except where permitted by law.

Figure 29

257. The PDF further purports to inform insureds about *all* of the ways in which their information, data, or searches may be disclosed:

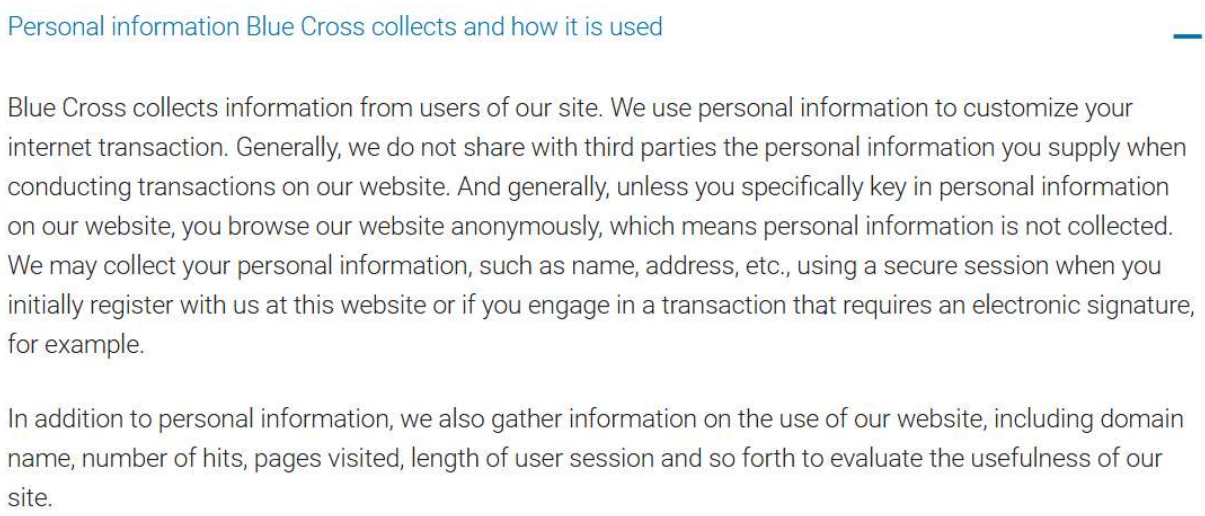
Any other use or disclosure of your protected health information, except as described in this Notice of Privacy Practices, will not be made without your signed authorization.

Figure 30[84]

258. It is only when insureds finally expand a text box under the Online Privacy Policy that any sort of tracking is generally disclosed for

[84] *Id.*

the first time, in contradiction to the HIPAA privacy policies and the misleadingly general web privacy statement:



Personal information Blue Cross collects and how it is used

Blue Cross collects information from users of our site. We use personal information to customize your internet transaction. Generally, we do not share with third parties the personal information you supply when conducting transactions on our website. And generally, unless you specifically key in personal information on our website, you browse our website anonymously, which means personal information is not collected. We may collect your personal information, such as name, address, etc., using a secure session when you initially register with us at this website or if you engage in a transaction that requires an electronic signature, for example.

In addition to personal information, we also gather information on the use of our website, including domain name, number of hits, pages visited, length of user session and so forth to evaluate the usefulness of our site.

Figure 31[85]

259. The disclosures provide that, "Generally, we do not share with third parties personal information you supply when conducting transactions on our website."

260. The disclosures falsely and misleadingly claim that information is gathered only "to evaluate the usefulness of our site" rather than for commercial purposes.

261. The disclosures also include vague and passive phrasing like "we may collect your personal information" or that "we also gather

[85] *Online Privacy Practices*, BCBSM, https://www.bcbsm.com/important-information/privacy-practices/, [https://perma.cc/VJK5-BNPE].

information." Additionally, it is buried in a long paragraph with generic and boilerplate language.

262. The disclosures fail to identify any specific Third-Party Vendors and instead refer to gathering information on the use of the Website that insureds could easily mistake for being Defendant's own trackers and not those of third parties.

263. The disclosures fail to specify what types of data are collected, or that the Tracking Technologies may use any cookies or other tools that can be used to identify, profile, or link insureds across multiple sessions or even the Internet. The disclosures do not refer to Session Replay Code that records insureds' entire sessions, including typed input, mouse movements, and navigations.

264. The disclosures fail to provide any opt out like a "reject" or "do not track" option.

265. The disclosures are not presented at the point of data collection, such as when an insured begins typing a sensitive medical condition.

266. Critically, the disclosures do not mention HIPAA rights.

267. Notably, the disclosures themselves and the above relevant subpages make heavy use of Tracking Technologies, with the Third-Party Vendors instantly tracking insureds' clicks and what they review. For instance, when insureds review the disclosure displayed in Figure 31 titled "Personal information Blue Cross collects and how it is used," Adobe collects this information and sends it back to its servers, instantly:

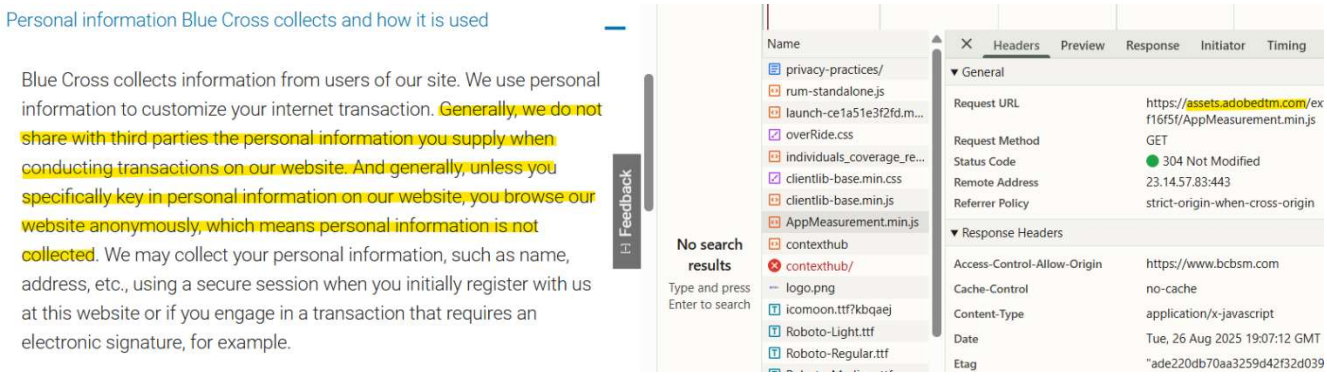


Figure 32

Figure 33

268. As shown in Figures 32 and 33, above, the insured is assigned a unique "visitor ID," as well as a "marketingCloudVisitorID," which are both provided to Adobe's Audience Management platform as the insured is assured by Defendant that he or she is browsing anonymously.

269. Insureds are not asked to consent prior to browsing Defendant's Website, and they are wiretapped from the moment they

load the site,[86] regardless of whether they eventually navigate to, download, read, or understand Defendant's "disclosures."

270. Defendant does not offer insureds any mechanism to meaningfully opt out of such data collection.

271. At no point does Defendant seek affirmative consent from insureds prior to the initiation of data tracking.

272. Valid consent to interception must be actual, informed, and voluntary.

273. In sum, the privacy policy on Defendant's Website is structured and worded to mislead users and to deflect attention from Defendant's impermissible, unlawful data collection through misleading general, and insufficient, obscure disclosures that require scrolling through (the information on several pages. It provides no explanation of the Tracking Technologies, no complete disclosure about the sharing of queries and sensitive information with third parties (including which third parties), and no way to opt out of data sharing.

[86] *Javier v. Assur. IQ, LLC*, No. 21-16351, 2022 U.S. App. LEXIS 14951, at *5 (9th Cir. May 31, 2022) (retroactive consent is not consent for digital wiretapping).

274. Insureds like Plaintiffs, who reasonably expect that their private health information that exists on a portal-based, secure healthcare website will remain confidential, are unaware that their keystrokes, searches, and clicks are being intercepted in real time. This does not and cannot constitute actual, informed, or voluntary consent.

275. In light of the above, Plaintiffs did not consent to Defendant's interception and collection of their Website Communications.

C. Defendant's Conduct Violates HIPAA's Privacy Rules.

276. Because Defendant's Website is branded under BCBSM, a health insurer, insureds have a reasonable expectation that their activity will remain private and secure.

277. Relatedly, courts and regulators have recognized that health-related data warrants elevated privacy protections due to its sensitivity and the risk of data misuse.

278. HIPAA's enhanced protections for health-related data support the conclusion that Plaintiffs had a reasonable expectation of privacy in interacting with Defendant's Website.

279. HIPAA prohibits business associates of covered entities like Defendant from using or disclosing PHI for purposes such as marketing, analytics, or other transmissions to third parties, unless the individual has provided a valid, written authorization. *See* 45 C.F.R. § 164.508(a)(3).

280. A valid HIPAA authorization must be written, specific, and signed by the individual. It must identify the data to be used or disclosed, the recipient, and the purpose. *See* 45 C.F.R. § 164.508(c)(1)(i)–(vi).

281. Defendant's integration of tracking technologies on its pages results in the automatic and unauthorized transmission of sensitive health-related data of the insureds of Defendant to third parties that include the Third-Party Vendors.

282. At no point did Defendant obtain HIPAA-compliant written authorizations from insureds before this transmission occurred.

283. The privacy policy on Defendant's Website does not provide the specificity, clarity, or accessibility legally required to satisfy HIPAA's notice and its authorization requirements.

284. Defendant's failure to transparently disclose its data practices, along with how insureds engage with the Defendant's Website, violates HIPAA's animating principle: Individuals must have control over their health information and be empowered to authorize or reject disclosures of such information.

285. By covertly transmitting insureds' interactions related to health services to third parties without authorization, Defendant has failed to meet the heightened duty of care owed to entities in possession of sensitive health information, as memorialized in HIPAA's statutory and regulatory regime.

286. In essence, Defendant failed in its core healthcare obligations by prioritizing marketing analytics and commercial gain over patient privacy.

D. The Applicable Statutes of Limitation Are Tolled.

287. None of the Plaintiffs were aware that their private health data were being intercepted and sent to the Third-Party Vendors.

288. None of the Plaintiffs consented to Defendant and the Third-Party Vendors intercepting their private health data.

289. Plaintiffs could not have, despite full diligence, discovered the full scope of Defendant's conduct as alleged herein, as there was no indication of the scope of the above-described tracking technology that Defendant employs on Defendant's Website.

290. Accordingly, the applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment and denial of the full scope of its use of these Tracking Technologies.

291. Defendant was under a duty to disclose the nature and extent of its data collection practices but did not do so.

292. Defendant is therefore estopped from relying on any statute of limitations defenses.

CLASS ACTION ALLEGATIONS

293. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23, individually and on behalf of a putative class of the following similarly situated individuals (collectively, the "Class"):

> Every current and former insured of Defendant whose Website Communications were captured from December 31, 2023 through the use of Tracking Technologies embedded in Defendant's Website, www.bcbsm.com,

including its subpages and patient portals, to the date of judgment herein.

294. **Numerosity:** The Class includes thousands of people, such that it is not practicable to join all Class members into one lawsuit.

295. **Commonality:** This case presents questions of law and fact that are common to the Class, including:

- Whether Defendant enables Third-Party Vendors to intercept the Website Communications of insureds to Defendant's Website, www.bcbsm.com, subpages, and insureds' portals, including the Main Portal, Prescription Portal, and Wellness Portal;
- Whether Defendant intentionally discloses the intercepted Website Communications of its insureds;
- Whether Defendant acquired the contents of insureds' Website Communications without their consent;
- Whether Defendant's conduct violates the FWA, Michigan's eavesdropping statute, and Michigan common law;
- Whether Plaintiffs and Class members are entitled to equitable relief; and

- Whether Plaintiffs and Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

296. **Typicality:** Plaintiffs, Class members, and Defendant have a commonality of interest in the subject matter of the lawsuit and the remedies sought.

297. **Predominance:** The common questions of law and fact predominate over any individual issue that may arise on behalf of an individual Class member.

298. **Superiority:** A class action is the appropriate vehicle for fair and efficient adjudication of the claims of Plaintiffs and Class members because if individual actions were required to be brought by each member of the Class, the result would be a multiplicity of actions, creating hardship to the Class, to the Court, and to Defendant.

299. **Adequacy of representation:** Plaintiffs and counsel will fairly and adequately protect the interests of Class members. Plaintiffs' lead counsel, Schlichter Bogard, will fairly and adequately represent the interests of the Class. Schlichter Bogard has a well-documented track record of successfully serving as class counsel in this Circuit and

elsewhere. Schlichter Bogard's pioneering work in class actions has been covered by numerous national publications, including the New York Times and Wall Street Journal, among other media outlets.

300. Schlichter Bogard has also been widely recognized by federal judges across the United States as pioneers in fiduciary breach class action litigation. Schlichter Bogard's vast experience in this area is reflected by the firm's appointment as class counsel in over 30 fiduciary breach class actions.

301. Federal judges have repeatedly recognized that Schlichter Bogard's efforts and successful outcomes have led to "enormous" savings for class members. *See e.g.*, *Cates v. Trs. of Columbia Univ.*, No. 16-6524, 2021 U.S. Dist. LEXIS 200890, at *15–16 (S.D.N.Y. Oct. 18, 2021).

302. Schlichter Bogard has additionally handled, and repeatedly prevailed in, fiduciary breach class action litigation in the U.S. Supreme Court. For example, in *Tibble v. Edison International*, a landmark fiduciary breach class action handled by Schlichter Bogard, after a partial loss in the U.S. District Court for the Central District of California, which was upheld by the U.S. Court of Appeals for the Ninth

Circuit, Schlichter Bogard achieved a reversal before the Supreme Court of the United States. The Supreme Court's vacatur in favor of the plaintiffs was unanimous. *See Tibble v. Edison Int'l*, 135 S. Ct. 1823 (2015).

303. Schlichter Bogard recently secured a reversal of a dismissal before the U.S. Supreme Court, again in a unanimous decision, in *Hughes v. Northwestern University* – another fiduciary breach class action. *See Hughes v. Nw. Univ.*, 595 U.S. 170 (2022).

304. In *Cunningham v. Cornell University*, yet another fiduciary breach class action, which was decided by the U.S. Supreme Court less than one month ago, Schlichter Bogard again achieved a unanimous victory. *See Cunningham v. Cornell Univ.*, 604 U.S. 693, 695 (2025).

305. Other courts have repeatedly heralded Schlichter Bogard's work in class action litigation. By way of limited example:

306. A U.S. district judge found as follows: "Class Counsel performed substantial work . . . investigating the facts, examining documents, and consulting and paying experts to determine whether it was viable. This case has been pending since September 11, 2006. Litigating the case required Class Counsel to be of the highest caliber

and committed to the interests of the [class]." *Will v. General Dynamics*, No. 06-698, 2010 U.S. Dist. LEXIS 123349, at *8–9 (S.D. Ill. Nov. 22, 2010).

307. "Schlichter, Bogard [] has achieved unparalleled results on behalf of its clients, . . . has invested . . . massive resources and persevered in the face of . . . enormous risks[.]" *Nolte v. Cigna*, No. 07-2046, 2013 U.S. Dist. LEXIS 184622, at *8 (C.D. Ill. Oct. 15, 2013) (obtaining recovery of $35 million on behalf of plan participants in Cigna's 401(k) plan).

308. "Litigating this case against formidable defendants and their sophisticated attorneys required Class Counsel to demonstrate extraordinary skill and determination." *Beesley v. Int'l Paper Co.*, No. 06-703, 2014 U.S. Dist. LEXIS 12037, at *8 (S.D. Ill. Jan. 31, 2014).

309. "Schlichter, Bogard [] demonstrated extraordinary skill and determination in obtaining this result for the Class." *Abbott v. Lockheed Martin Corp.*, No. 06-701, 2015 U.S. Dist. LEXIS 93206, at *9 (S.D. Ill. July 17, 2015).

CAUSES OF ACTION

COUNT I – VIOLATION OF FEDERAL WIRETAP ACT, 18 U.S.C. § 2510 et seq.

(ON BEHALF OF PLAINTIFFS AND THE CLASS)

310. Plaintiffs incorporate the preceding paragraphs as though fully realleged herein.

311. The FWA gives a private right of action to anyone whose communications are intercepted, disclosed, or used in violation of the statute. 18 U.S.C. § 2520(a).

312. The FWA, as amended by the ECPA, prohibits any person from intentionally intercepting, disclosing, or using the contents of any wire, oral, or electronic communication without consent or as otherwise permitted by law.

313. The FWA, as amended by the ECPA, extends wiretap protections to digital transmissions, including those alleged herein.

314. Plaintiffs' interactions and Website Communications with Defendant's Website are "electronic communications" under 18 U.S.C. § 2510(12), and the information they contain constitutes "contents" under 18 U.S.C. § 2510(8).

315. Defendant, through Tracking Technologies and tracking code embedded on its Website, intentionally intercepted these Website Communications such that they were disclosed to the Third-Party Vendors without Plaintiffs' knowledge or valid, informed consent.

316. Any alleged one-party consent by Defendant is invalid because Defendant committed a federal crime of "knowingly" disclosing "individually identifiable health information" to third parties. 42 U.S.C. § 1320d–6(a),

317. Any alleged one-party consent by Defendant is invalid because the Defendant committed torts as outlined herein like intrusion upon seclusion.

318. As a result, the FWA's consent exception is void under the FWA and Defendant is liable for damages. 18 U.S.C. § 2511(2)(d).

319. Plaintiffs request the relief set forth in the Request for Relief below.

COUNT II – VIOLATION OF MICHIGAN EAVESDROPPING STATUTE, MCL 750.539a et seq.

(ON BEHALF OF PLAINTIFFS AND THE CLASS)

320. Plaintiffs incorporate the preceding paragraphs as though fully realleged herein.

321. Michigan's eavesdropping statute, MCL 750.539c, prohibits the willful use of any device to eavesdrop upon, record, or transmit a private conversation without the consent of all parties.

322. "Eavesdrop" is defined broadly under MCL 750.539a(2) to mean overhearing, recording, amplifying, or transmitting any part of the private discourse of others without the consent of all parties.

323. Defendant intentionally embedded Tracking Technologies from the Third-Party Vendors that operated as "devices" under Michigan's eavesdropping statute. These Tracking Technologies captured, recorded, and transmitted the exact content of Plaintiffs' Website Communications to third-party servers in real time.

324. These Website Communications, including searches for sensitive medical conditions, entries of geographic identifiers to locate providers, and other keystrokes, constitute "private conversations" within the meaning of Michigan's eavesdropping statute. Plaintiffs reasonably expected that these Website Communications would only be viewed by Defendant in its capacity as their insurer, not disclosed to or intercepted by unrelated third parties and the Third-Party Vendors.

325. Defendant's conduct constitutes "eavesdropping" within the meaning of MCL 750.539a(2) because the interception and transmission of Website Communications to the Third-Party Vendors occurred without the consent of all parties to the conversations.

326. Plaintiffs did not consent to such interception and transmission as it occurred immediately upon Plaintiffs' visits to the Website and without their knowledge. Liability under Michigan's eavesdropping statute attaches at the moment of the interception.

327. Furthermore, Plaintiffs did not consent because the buried and misleading privacy statements on the Website did not provide clear, informed, and voluntary consent required by Michigan's eavesdropping statute.

328. As a direct and proximate result of Defendant's unlawful conduct, Plaintiffs and the Class members have suffered injury, including loss of privacy, exposure of sensitive health-related information, and loss of control over their personal data.

329. Plaintiffs request the relief set forth in the Request for Relief below, including actual and punitive damages pursuant to MCL 750.539h.

COUNT III – BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

330. Plaintiffs incorporate the preceding paragraphs as though fully realleged herein.

331. As a covered entity under HIPAA, Defendant had a fiduciary duty to maintain the confidentiality and privacy of Plaintiffs' personal health information, including the Website Communications made on Defendant's Website.[87]

332. Concurrently, as a business associate of a covered entity under HIPAA, Defendant had a fiduciary duty to maintain the confidentiality and privacy of Plaintiffs' personal health information, including the Website Communications made on Defendant's Website.[88]

333. Defendant likewise had a fiduciary duty, under Michigan law, to ensure the confidentiality of patient data, including MCL 333.20175, MCL § 550.1406, and MCL 333.26261–333.26271, which mandate that medical records and patient data be treated as confidential.

[87] 145 C.F.R. § 164.502 (uses and disclosures of protected health information).
[88] 145 C.F.R. § 164.502 (uses and disclosures of protected health information).

334. Defendant's fiduciary duty extended to ensuring that any collection, use, or sharing of personal health information was done only with the specific informed consent of the individual from whom the information was collected.[89]

335. At all relevant times, a relationship existed between Plaintiffs and Defendant, in which Plaintiffs entrusted Defendant to protect the private and personal health information of Plaintiffs and members of the putative Class, and Defendant accepted that trust.[90]

336. Defendant breached the fiduciary duty that it owed to Plaintiffs and the putative Class by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect, or intentionally disclosing, this private

---

[89] *Id.*

[90] *In re Karmey Estate*, 468 Mich. 68, 74 n.2 (2003) (adopting the Black's Law Dictionary definition of "fiduciary relationship" and defining it as, "(1) when one person places trust in the faithful integrity of another, who as a result gains superiority or influence over the first, (2) when one person assumes control and responsibility over another, (3) when one person has a duty to act for or give advice to another on matters falling within the scope of the relationship, or (4) when there is a specific relationship that has traditionally been recognized as involving fiduciary duties, as with a lawyer and a client or a stockbroker and a customer.").

and personal health information, while deliberately concealing their breaches from Plaintiffs.[91]

337. Defendant's actions in enabling the interception and transmission of Plaintiffs' sensitive health information without informed consent constitutes a breach of the fiduciary duty that Defendant owes to Plaintiffs and the Class members under Michigan law.[92]

338. Defendant breached its fiduciary duty by failing to "subordinate" its interests in marketing and tracking Plaintiffs' private health-related information to the privacy interests of Plaintiffs.[93]

339. As a direct result of Defendant's actions, Plaintiffs and the Class members have suffered harm, including but not limited to the unauthorized disclosure of their highly sensitive private health information, the risk of identity theft, and other potential damage

---

[91] "Under Michigan law, 'a fiduciary relationship arises from the reposing of faith, confidence, and trust and the reliance of one on the judgment and advice of another.'" *Petroleum Enhancer, LLC v. Woodward*, 690 F.3d 757, 765–66 (6th Cir. 2012) (quoting *Teadt v. Lutheran Church Mo. Synod*, 237 Mich. App. 567, 580-81 (1999)).

[92] *Delphi Auto PLC v Absmeier*, 167 F. Supp. 3d 868, 884 (E.D. Mich. 2016).

[93] A fiduciary must "subordinat[e] one's personal interests to that of the other person." *Wallad v. Access BIDCO, Inc.*, 236 Mich. App. 303, 307 (Mich. Ct. App. 1999).

arising from the unauthorized collection and sharing of personal health data.

340. Plaintiffs request the relief set forth in the Request for Relief below.

COUNT IV – INTRUSION UPON SECLUSION
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

341. Plaintiffs incorporate the preceding paragraphs as though fully realleged herein.

342. Under Michigan law, the tort of intrusion upon seclusion occurs when there is "(1) the existence of a secret and private subject matter; (2) a right possessed by the plaintiff to keep that subject matter private; and (3) the obtaining of information about that subject matter through some method objectionable to a reasonable man."[94]

343. Plaintiffs and the Class members had a reasonable expectation of privacy in their interactions with Defendant's Website, including the Website Communications, which includes their search queries and page visits relating to their personal conditions and potential treatments.

[94] *Doe. v. Mills*, 212 Mich. App. 73, 88 (1995) (citing *Tobin v. Civil Service Comm'n*, 416 Mich. 661, 672 (1982)).

344. Plaintiffs and the Class members had a specific right enshrined by HIPAA and Michigan statutes protecting the confidentiality of medical records to keep that medical information private.

345. Defendant's Website purports to offer security for accessing such health information.

346. However, without Plaintiffs' or the Class members' knowledge or consent, Defendant embedded Tracking Technologies (including those from the Third-Party Vendors) on the Website to record and transmit Website Communications in real time.

347. Defendant deliberately intruded into Plaintiffs' and the Class members' private affairs, in a way that a reasonable person would find highly offensive, especially given that the Defendant failed to disclose the extent of the Tracking Technologies and made misrepresentations that insureds' information would remain confidential.

348. In so doing, Defendant egregiously violated Michigan's privacy norms and legal protections.

349. As a direct and proximate result of Defendant's actions, Plaintiffs and the Class members suffered and continue to suffer injuries, including loss of privacy, exposure to increased risk of identity theft, and loss of control over their private data.

350. Plaintiffs request the relief set forth in the Request for Relief below.

COUNT V – UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

351. Plaintiffs incorporate the preceding paragraphs as though fully realleged herein.

352. Under Michigan law, unjust enrichment occurs when the defendant received a benefit from a plaintiff and retention of that benefit under the circumstances is inequitable to the plaintiff.[95]

353. Defendant obtained a significant financial benefit by covertly collecting, using, and sharing the personal health-related data of Plaintiffs and the Class members with third parties, including the Third-Party Vendors, without consent.

[95] *Barber v SMH (US), Inc*, 202 Mich. App. 366, 375 (1993).

354. Defendant has been unjustly enriched by using this sensitive health information, which has enormous value, to generate profits through targeted advertising and the sale or use of the data by third parties, including the Third-Party Vendors.

355. By collecting and transmitting these data without providing adequate notice or obtaining informed consent, Defendant has exploited the private health information of Plaintiffs for illicit financial gain, in violation of principles of fairness and equity.

356. In contrast, Plaintiffs and the Class members have suffered harm, including the loss of privacy and the potential for identity theft.

357. Defendant's conduct is inequitable because it is unfair for a business associate of a covered entity, who owes a fiduciary duty to protect the privacy and confidentiality of patients' health data, to harvest and profit from that information without consent.

358. The benefits that Defendant derived from Plaintiffs and the Class members rightly belong to Plaintiffs and the Class members, as it is their private health information.

359. It would be inequitable under unjust enrichment principles for Defendant to retain any of the profits or other benefits derived from the practices alleged in this Complaint.

360. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs all unlawful or inequitable proceeds received as a result of the conduct alleged in this Complaint.

REQUEST FOR RELIEF

Plaintiffs, on behalf of themselves and the Class, request judgment against Defendant as follows:

A. Certifying this case as a class action, appointing Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class counsel for the Class;

B. Finding that Defendant's conduct violates the FWA, Michigan's eavesdropping statute, and Michigan common law;

C. Awarding actual damages caused by Defendant's violations of the FWA, Michigan's eavesdropping statute, and Michigan common law;

D. Awarding statutory damages as provided under 18 U.S.C. § 2520, including the greater of $10,000 of $100 per day for each violation of the FWA;

E. Awarding damages as otherwise provided under Michigan's eavesdropping statute, including punitive damages, injunctive relief, and reasonable attorney's fees and costs;

F. Awarding compensatory damages, restitution, disgorgement, attorneys' fees and costs, and/or punitive damages as permitted by law and as the Court deems just and proper;

G. Entering equitable relief enjoining Defendant from engaging in the misuse and/or disclosure of Plaintiffs' and Class members' data, and the issuance of prompt, complete and accurate disclosures to Plaintiffs, Class members, and all current and future users of the Website;

H. Entering equitable relief requiring restitution and disgorgement of any profits wrongfully obtained as a result of Defendant's wrongful conduct;

I. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

J. Awarding such other and further relief as this Court deems appropriate and as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the Class, request trial by jury of all claims asserted herein.

December 31, 2025

Respectfully submitted,

/s/ R.J. Cronkhite
R.J. Cronkhite (P78374)
Cronkhite Counsel PLLC
36800 Woodward Ave., Suite 310
Bloomfield Hills, MI 48304
T: (248) 309-8601
F: (248) 256-2555
rj@cronkhitelaw.com

Local Counsel for Plaintiffs

SCHLICHTER BOGARD LLC
Andrew D. Schlichter*
Alexander L. Braitberg*
Chen Kasher*
Cort VanOstran*
100 South Fourth Street, Suite 1200
St. Louis, MO 63102
(314) 621-6115
(314) 621-5934 (fax)
aschlichter@uselaws.com
abraitberg@uselaws.com
ckasher@uselaws.com
cvanostran@uselaws.com

*Application for admission
forthcoming

Attorneys for Plaintiffs