UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

Teresa Gouch, Denise Spanos, George Amerson, Kyle Mummey, and Marcia Beasley, individually and on behalf of themselves and all others similarly situated, Plaintiffs, v. Blue Cross Blue Shield Association, Defendant.	Case No. **CLASS ACTION COMPLAINT** Jury Trial Demanded

Plaintiffs ("Plaintiffs"), on behalf of themselves and all others similarly situated, file this Class Action Complaint against Defendant Blue Cross Blue Shield Association ("Defendant" or "BCBS"), and in support state the following:

INTRODUCTION

1. This case is about the serious privacy and national security threat posed by Defendants' unauthorized disclosure of federal employees' sensitive medical information to third parties, including the China-owned social media company, TikTok.

2. Through a contract with the federal government, BCBS provides health insurance to over 5.5 million federal employees, retirees, and their families across the U.S. and overseas.[1] This includes employees at all levels of the executive and judicial branches of the government. Given its role as the largest health insurance provider for the federal workforce, Defendant has access to vast amounts of sensitive medical information.

[1] https://www.fepblue.org/about-us

3. As part of its offerings to federal employees, Defendant operates a website, www.fepblue.org, (the "Website"), where it allows federal employees to shop for insurance plans, find doctors, and research specific symptoms and conditions, such as "Mental Health" and "Pregnancy."

4. Unbeknownst to the federal employees visiting the Website, BCBS allows third-party technology companies, including TikTok, to secretly intercept and record the employees' communications and activities on the Website in real-time, including specific searches for sensitive health-related topics. Defendant does this despite the U.S. government's far-reaching efforts to prevent the disclosure of sensitive government information to TikTok by banning the popular social media app on official government devices and systems.

5. Plaintiffs bring this class action complaint on behalf of a class of federal employees, retirees, and their family members (collectively "federal employees") impacted by Defendant's secret and unauthorized disclosure of their highly sensitive Personal Health Information ("PHI") and Personally Identifiable Information ("PII") (collectively "Sensitive Information") to TikTok and other third parties.

6. Given widespread concerns in recent years over TikTok's aggressive data-collection practices and the company's close ties to China, TikTok has been banned on official government devices for Members of the U.S. House of Representatives, executive branch employees, and federal contractors. Citing privacy and security concerns, state and local governments across the U.S. have likewise banned TikTok on official government devices. Multiple countries across the globe have taken similar actions.

7. Despite the widespread privacy and national security concerns associated with TikTok, BCBS inexplicably deployed tracking code from TikTok and other technology companies

on its Website to secretly intercept and record federal employees' online communications regarding sensitive health-related topics.

8. In December 2022, the U.S. Department of Health and Human Services Office for Civil Rights warned healthcare entities that, "Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."[2] The OCR's guidance also made clear that, "disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures."[3]

9. More recently, in July 2023, federal regulators sent a letter to approximately 130 healthcare providers warning them about the use of online tracking technologies that could result in unauthorized disclosures of Sensitive Information to third parties.[4] The letter highlighted the "risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities," and warned about "[i]mpermissible disclosures of an individual's personal health information to third parties" that could "result in a wide range of harms to an individual or others."[5] According to the letter, "[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more."[6]

---

[2] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

[3] *Id.*

[4] https://www.ftc.gov/business-guidance/blog/2023/07/ftc-hhs-joint-letter-gets-heart-risks-tracking-technologies-pose-personal-health-information

[5] https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

[6] *Id.*

10. Despite these warnings from federal regulators, Defendant BCBS deployed tracking technologies that allowed third-party social technology companies, such as TikTok, to intercept federal employees' communications with BCBS and use the data to sell targeted advertising and/or otherwise monetize the data in the ever-growing marketplace for PII and PHI. Defendant also made use of the intercepted information for targeted advertising and marketing campaigns through TikTok and other third-party advertisers, as well as for its own data analytics.

11. As a provider of health insurance, Defendant had a duty to maintain the security and privacy of federal employees' Sensitive Information and prevent unauthorized disclosure of that information to third-party technology companies like TikTok. Defendant breached that duty by deploying the tracking code from TikTok and other companies on its Website, which resulted in the interception of Plaintiffs' and the Class's Sensitive Information by unauthorized third parties.

12. Defendant's disclosure of Sensitive Information allowed TikTok and other third parties to identify and know that specific federal employees were seeking confidential medical care or were being treated for a specific condition.

13. Plaintiffs and the Class never consented to, authorized, or otherwise agreed to allow Defendant to disclose their Sensitive Information to anyone other than those reasonably believed to be part of BCBS, acting in some healthcare capacity.

14. As a direct and proximate result of Defendant's unauthorized disclosure of Plaintiffs' and the Class's Sensitive Information, Plaintiffs and the Class Members have suffered injury and harm, including invasions of privacy associated with the loss of their sensitive medical data; emotional distress; loss of the benefit of the bargain Plaintiffs and the Class considered at the time they bargained for health insurance services and agreed to use Defendant's Website; statutory

damages; and the imminent and ongoing substantial risk of their Sensitive Information being exposed to third parties.

15. Plaintiffs and the Class bring this action to recover for the harm they suffered and assert the following claims: violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2511; violations of the Illinois Eavesdropping Statute, 720 ILCS § 5/14-1, *et seq.*; violations of the Illinois Computer Tampering Act, 720 ILCS § 5/17-51; violations of the California Invasion of Privacy Act, Cal. Penal Code § 630, *et seq.*; Negligence; Invasion of Privacy; Breach of Implied Contract; and Unjust Enrichment.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because the Complaint asserts claims pursuant to Defendant's violations of ECPA, 18 U.S.C. § 2511.

17. This Court also has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

18. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

19. Venue is proper under 18 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in this District.

PARTIES

20. **Plaintiff** Teresa Gouch is a resident of California. At all relevant times, Plaintiff

Gouch was a federal employee who received health insurance from Defendant under the Federal Employee Program. Plaintiff Gouch maintained accounts with TikTok, Facebook, Instagram, and Google, and remained logged in to her accounts when browsing the internet. From approximately 2020 to the present, Plaintiff Gouch visited Defendant's Website while in California using her personal computer and cell phone to search for doctors, including by typing words into the Website's "search" bar, and to research specific health conditions.

21. **Plaintiff** Denise Spanos is a resident of South Carolina. At all relevant times, Plaintiff Spanos was a retired federal employee who received health insurance from Defendant under the Federal Employee Program. Plaintiff Spanos maintained accounts with TikTok, Facebook, Instagram, and Google, and remained logged in to her accounts when browsing the internet. Plaintiff Spanos also maintained a LinkedIn account but did not remain logged in. For many years and up to the present, Plaintiff Spanos visited Defendant's Website while in South Carolina using her personal computer or cell phone to search for prescription information, health plan information, and health assessments, including by typing words into the Website's "search" bar in order to find relevant subpages on the Website. Plaintiff Spanos also used the Website to search for doctors.

22. **Plaintiff** George Amerson is a resident of Texas. At all relevant times, Plaintiff Amerson was a federal employee who received health insurance from Defendant under the Federal Employee Program. Plaintiff Amerson maintained accounts with TikTok, Facebook, Instagram, LinkedIn, and Google, and remained logged in to his accounts when browsing the internet. For many years and up to the present, Plaintiff Amerson visited Defendant's Website while in Texas using his personal computers and cell phone to search for doctors, including by typing words into the Website's "search" bar.

23. **Plaintiff** Kyle Mummey is a resident of Pennsylvania. At all relevant times, Plaintiff Mummey was a federal employee who received health insurance from Defendant under the Federal Employee Program. Plaintiff Mummey maintained accounts with TikTok, Facebook, Instagram, LinkedIn, and Google, and remained logged in to his accounts when browsing the internet. From approximately December 2021 to the present, Plaintiff Mummey visited Defendant's Website while in Pennsylvania using his personal computer to search for doctors, research symptoms and conditions, and shop for health insurance plans.

24. **Plaintiff** Marcia Beasley is a resident of Florida. At all relevant times, Plaintiff Beasley was a retired federal employee who received health insurance from Defendant under the Federal Employee Program. Plaintiff Beasley maintained accounts with TikTok, Facebook, Instagram, LinkedIn, and Google, and remained logged in to her TikTok, Facebook, and Google accounts when browsing the internet. For many years and up to 2022, Plaintiff Beasley visited Defendant's Website while in Florida using her personal computer and cell phone to search for doctors, research symptoms and conditions, and inquire about prescriptions, including by typing words into the Website's "search" bar.

25. Plaintiffs reasonably expected that their online communications with Defendant were between them and Defendant, would remain private, and would not be shared with third parties without their consent.

26. After using Defendant's website, most Plaintiffs recall receiving online ads from BCBS. Plaintiff Mummey recalls receiving ads from BCBS on Facebook and TikTok related to information he searched for on Defendant's Website.

27. **Defendant** Blue Cross Blue Shield Association is an Illinois corporation with its principal place of business in Chicago, Illinois. According to its website, the "Blue Cross Blue

Shield Association is a national association of 34 independent, community-based and locally operated Blue Cross Blue Shield companies. The Association owns and manages the Blue Cross and Blue Shield trademarks and names in more than 170 countries around the world. The Association also grants licenses to independent companies to use the trademarks and names in exclusive geographic areas."[7]

28. The Blue Cross Blue Shield Association also administers the Federal Employee Program, which provides health insurance to the federal workforce through BCBS's 34 community-based companies.[8] The Blue Cross Blue Shield Association negotiates annually with the U.S. Office of Personnel Management to determine the benefits and premiums for the Federal Employee Program.[9] BCBS's statutory agent is Scott Nehs, 225 N. Michigan Ave., Chicago, IL 60601.

FACTUAL BACKGROUND

A. TikTok's Campaign to Harvest Personal Data on U.S. Citizens

29. TikTok is a social media company owned by Chinese tech giant, ByteDance, which has been called "the world's most valuable startup."[10] In 2021, ByteDance boasted $58 billion in revenue and 1.9 billion monthly active users.[11]

[7] https://www.bcbs.com/about-us/the-blue-cross-blue-shield-system

[8] https://www.fepblue.org/about-us

[9] *Id.*

[10] https://hbr.org/2022/02/how-bytedance-became-the-worlds-most-valuable-startup

[11] *Id.*

30. TikTok is ByteDance's most popular product, which itself has over 150 million American users,[12] and has been downloaded over 3 billion times globally.[13]

31. Like many social media companies, TikTok makes most of its revenue from advertising.[14] In 2022, TikTok's advertising revenue topped $9.9 billion.[15] While TikTok currently trails social media giant Meta in terms of users and ad revenue,[16] TikTok's increasing popularity is reflected by the fact that "its average user in the U.S. spends more time with the service than with Facebook and Instagram put together."[17] Indeed, a recent survey found that "[t]wo-thirds of American teens use TikTok every day . . . with 16% saying they're on the platform almost constantly."[18]

32. TikTok's explosive growth is due in large part to its proprietary algorithm,[19] which harvests massive amounts of user data and targets users with highly tailored videos and content.[20] TikTok gathers data about when users arrive on its site (even if not signed up), and once a user does sign up, TikTok gathers detailed information about all activities within the app, including "the device you are using, your location, IP address, search history, the content of your messages,

[12] https://apnews.com/article/tiktok-bytedance-shou-zi-chew-8d8a6a9694357040d484670b7f4833be

[13] https://hbr.org/2022/02/how-bytedance-became-the-worlds-most-valuable-startup

[14] https://www.wsj.com/articles/tiktok-struggling-with-slowing-digital-advertising-industry-lowers-ad-revenue-outlook-11668139787

[15] https://www.shopify.com/blog/tiktok-ad-spending

[16] *Id.*

[17] https://www.bloomberg.com/news/newsletters/2022-06-28/how-does-tiktok-make-money-app-relies-on-a-few-main-ingredients

[18] https://www.washingtonpost.com/business/2023/06/09/how-tiktok-became-a-us-china-national-security-issue/9a158cca-06da-11ee-b74a-5bdd335d4fa2_story.html

[19] https://www.bloomberg.com/news/newsletters/2022-06-28/how-does-tiktok-make-money-app-relies-on-a-few-main-ingredients

[20] https://www.theguardian.com/technology/2022/jul/19/tiktok-has-been-accused-of-aggressive-data-harvesting-is-your-information-at-risk

what you're viewing and for how long[,] and device identifiers to track your interactions with advertisers."[21] TikTok also "infers factors such as your age range, gender and interests based on the information it has about you," and "can collect biometric information including face and voiceprints."[22]

33. TikTok's aggressive data-harvesting practices have resulted in fines and settlements in recent years. In 2019, the Federal Trade Commission fined TikTok $5.7 million for violating the privacy of children under the age of 13 who used the app.[23] In 2021, TikTok agreed to pay $92 million to settle claims in the U.S. that it illegally "harvested personal data from users, including information using facial recognition technology, without consent and shared the data with third-parties, some of which were based in China."[24] TikTok was also recently sued in a class action complaint alleging that TikTok unlawfully collects data on non-TikTok users who browse the internet. The Court has denied TikTok's motion to dismiss most of the class's claims.[25]

B. Governments Ban TikTok on Official Devices Out of Security Concerns

34. Given TikTok's aggressive data-harvesting practices and its direct ties to China, government entities in the U.S. and across the globe have taken steps to ban the use of TikTok on official government devices. The movement stems from concerns that TikTok, as a subsidiary of

[21] https://www.wired.co.uk/article/tiktok-data-privacy

[22] *Id.*

[23] https://www.nbcnews.com/tech/tech-news/tiktok-pay-5-7-million-over-alleged-violation-childprivacy-n977186

[24] https://www.npr.org/2021/02/25/971460327/tiktok-to-pay-92-million-to-settle-class-action-suit-over-theft-of-personal-data

[25] *Griffith v. TikTok, Inc.*, 23-cv-00964-SB-E (C.D.C.A. Oct. 6, 2023) (ECF No. 59).

China-based ByteDance, is controlled by or would be forced to share information with the Chinese government.[26]

35. Despite TikTok's efforts to publicly distance itself from China,[27] recent reporting confirms that ByteDance exercises close control over TikTok's operations. Since the beginning of 2023, "a string of high-level executives have transferred from ByteDance to TikTok, taking on some of the top jobs" after relocating from "ByteDance's Beijing headquarters."[28] The ByteDance executives "have taken on roles overseeing swaths of TikTok's advertising business, human resources, monetization, business marketing and products related to advertising and e-commerce initiatives. Some have brought teams from Beijing."[29]

36. The concerns over TikTok's close ties to China are widespread and bipartisan. In December 2022, the U.S. House of Representatives banned TikTok from all House-managed mobile devices citing "a number of security risks."[30]

37. In February 2023, the White House announced that "all federal agencies must eliminate TikTok from phones and systems and prohibit internet traffic from reaching the company."[31] The Office of Management and Budget called the directive a "critical step forward

[26] https://apnews.com/article/tiktok-bytedance-shou-zi-chew-8d8a6a9694357040d484670b7f4833be

[27] https://www.wsj.com/articles/tiktoks-efforts-to-cut-ties-with-chinese-parent-stumble-over-talent-11671186110

[28] https://www.wsj.com/tech/tiktok-employees-say-executive-moves-to-u-s-show-china-parents-influence-ef5ff21f?mod=hp_lead_pos1

[29] *Id.*

[30] https://www.cbsnews.com/news/tiktok-ban-government-devices-house-of-representatives-congress/

[31] https://www.reuters.com/technology/white-house-gives-agencies-30-days-impose-federal-device-tiktok-ban-2023-02-27/

in addressing the risks presented by the app to sensitive government data."[32] The agency's Chief Information Security Officer added that, "[t]he Biden-Harris Administration has invested heavily in defending our nation's digital infrastructure and curbing foreign adversaries' access to Americans' data," and noted that the ban "is part of the Administration's ongoing commitment to securing our digital infrastructure and protecting the American people's security and privacy."[33]

38. In March 2023, the Director of the FBI warned Congress that China's government could use TikTok to control data on millions of American users and that the app "screams" of security concerns.[34] The Director of the National Security Agency expressed similar security concerns in congressional testimony.[35]

39. In June 2023, the U.S. government extended the TikTok ban to electronic devices used by all federal contractors.[36]

40. State and local governments across the U.S. have also banned TikTok on official government devices and systems.[37] In August 2023, for example, New York City "joined a wave of states and federal agencies in banning TikTok from government-owned devices based on security concerns."[38]

---

[32] https://apnews.com/article/technology-politics-united-states-government-ap-top-news-business-95491774cf8f0fe3e2b9634658a22e56

[33] https://www.axios.com/2023/02/28/white-house-federal-agencies-remove-tiktok

[34] https://www.reuters.com/technology/fbi-chief-says-tiktok-screams-us-national-security-concerns-2023-03-08/

[35] https://www.reuters.com/world/us/us-nsa-director-concerned-by-tiktok-data-collection-use-influence-operations-2023-03-07/

[36] https://www.nationaldefensemagazine.org/articles/2023/6/26/just-in-tiktok-ban-issued-for-federal-government-contractors

[37] https://www.nlc.org/article/2023/02/06/what-the-national-and-state-tiktok-bans-mean-for-local-governments/

[38] https://www.nytimes.com/2023/08/16/technology/tiktok-ban-new-york-city.html

41. Congress is also considering legislation that would give the President authority to ban TikTok nationwide,[39] although that legislation has lost some momentum recently in the wake of a $100 million lobbying effort by TikTok[40] that involves dark money spending and a high-level influence campaign.[41]

42. Governments outside the U.S.—including Canada, the U.K., France, Australia, and many others—have also taken note of TikTok's security and privacy concerns, banning TikTok from government devices and systems.[42]

43. With a growing wave of government bans on the use of the TikTok app, TikTok has turned to another data-harvesting mechanism that secretly operates across the internet and does not require a user to download or use the app: the TikTok Pixel.

C. The TikTok Pixel Intercepts and Records Internet Communications

44. Like other social media companies, TikTok's advertising revenue flows from its ability to sell highly targeted and curated advertisements. To target and curate advertising campaigns, TikTok relies on the massive trove of data it extracts from its users who interact with the app. But TikTok also harvests data from the internet at large, deploying the TikTok Pixel to follow individuals around as they browse the internet and intercept their online communications.[43]

[39] https://www.nbcnews.com/politics/congress/congress-tiktok-ban-social-media-%2027harms-teens-rcna70998

[40] https://www.reuters.com/technology/us-lawmakers-considering-changes-tiktok-bill-senator-2023-07-10/

[41] https://www.wsj.com/politics/policy/jeff-yass-tiktok-bytedance-ban-congress-15a41ec4

[42] https://apnews.com/article/tiktok-ban-privacy-cybersecurity-bytedance-china-2dce297f0aed056efe53309bbcd44a04

[43] https://www.consumerreports.org/electronics-computers/privacy/tiktok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/

45. The TikTok Pixel's "proliferation offers another vector for data collection beyond TikTok's popular mobile app, which is increasingly under fire in Washington as a possible way for the Chinese government to collect data on Americans."[44]

i. Background on internet communications

46. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as 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).

47. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

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

a. HTTP Request: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies. POST Requests can send a large amount of data outside of the URL (for instance, uploading a PDF for filing a motion to a court).

[44] https://www.wsj.com/articles/tiktok-trackers-embedded-in-u-s-state-government-websites-review-finds-a2589f0

b. Cookies: a small text file that can be used to store information on the client device that can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.

c. HTTP Response: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

49. An individual's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as a specific webpage). The HTTP Response sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the individual's screen as they navigate a website.

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

51. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the user of the web browser. When the TikTok Pixel is embedded in a website's Source Code, it causes the user's web browser to simultaneously transmit communications directed to the website to also go to TikTok's servers. In this way, TikTok is able to intercept a user's online communications with a website where the TikTok pixel is embedded.

ii. The TikTok Pixel

52. The TikTok Pixel is a piece of code that companies can embed in their websites to transmit information to TikTok about user activities on the website.[45] Once the TikTok Pixel is installed on a website, the Pixel secretly operates in the background, invisible to visitors to the website, while it intercepts and records the user's communications with the website.

53. By default, the TikTok Pixel collects the following information: the timing of when actions on the website take place (like when a page is viewed); the user's IP address; the device make, model, operating system, and browser information for the user; third-party cookies to match the user's website communications to an identified person on TikTok; pages viewed on the website; buttons clicked on the website; and content typed into "search" bars.[46] Beyond these standard collection efforts, a website owner can also customize the TikTok Pixel to collect additional information about a website visitor's activities and transmit that information to TikTok.[47]

54. Because the TikTok Pixel is invisible to the website visitor, the data collection occurs without the visitor's knowledge or consent.

55. By secretly recording and transmitting data to TikTok—without the user's knowledge or consent—the TikTok Pixel acts much like a traditional wiretap. When individuals visit a website via an HTTP Request to the website's server, the server sends an HTTP Response including the Markup that displays the webpage visible to the user along with the invisible Source Code that includes the TikTok Pixel. At that point, the website owner, in essence, hands individuals visiting its website a tapped device. Once the webpage is loaded into the individual's

[45] https://ads.tiktok.com/help/article/tiktok-pixel

[46] *Id.*; *see also* https://ads.tiktok.com/help/article/standard-events-parameters?lang=en

[47] https://ads.tiktok.com/help/article/standard-events-parameters?lang=en

browser, the TikTok Pixel quietly waits for private user communications on the webpage to trigger the code-based wiretap. The TikTok Pixel then simultaneously intercepts those communications intended only for Defendant and transmits the communications to TikTok.

iii. TikTok Matches the User's Internet Communications to an Identified Individual

56. TikTok uses cookies and other unique identifiers intercepted by the TikTok Pixel to match a website visitor's communications and activities with a particular individual.

57. When an individual with a TikTok account visits a website that uses the TikTok Pixel, the Pixel intercepts the individual's communications and transmits them to TikTok along with unique first and third-party cookies. TikTok can then "match[] [the] visitors on [the] website with people on TikTok."[48]

58. Even when an individual does not have a TikTok account, when they visit a website that uses the TikTok Pixel, the Pixel intercepts the individual's communications and transmits the information to TikTok.[49] On information and belief, TikTok can then match the communications to a particular individual through a process called "fingerprinting."[50]

59. The process of "fingerprinting" has been described as follows:

> The exact configuration of lines and swirls that make up your fingerprints are thought to be unique to you. Similarly, your browser fingerprint is a set of information that's collected from your phone or laptop each time you use it that advertisers can eventually link back to you. It takes information about your browser, your network, your device and combines it together to create a set of characteristics that is mostly unique to you.[51]

---

[48] https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?redirected=2

[49] https://www.consumerreports.org/electronics-computers/privacy/tiktok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/

[50] https://www.wired.com/story/browser-fingerprinting-tracking-explained/

[51] *Id.*

60. "By combining all this information into a fingerprint, it's possible for advertisers to recognize you as you move from one website to the next. Multiple studies looking at fingerprinting have found that around 80 to 90 percent of browser fingerprints are unique."[52] In addition, "[o]nce established, someone's fingerprint can potentially be combined with other personal information—such as linking it with existing profiles or information murky data brokers hold about you."[53]

61. A job posting for TikTok's Ads Signals team highlights TikTok's objective of harvesting consumer data from the internet at large. The posting states that the "team's vision is to understand customers' behavior by collecting their online/*offline activity* from varied sources and connecting them across devices using robust Identity graph in a privacy compliant way."[54] An identity graph "is a database that houses all the known identifiers that correlate with individual customers. Across a consumer's journey, one or many personal identifiers may be associated with an individual — email addresses, a physical address, mobile phone numbers, device IDs, account usernames, customer IDs, loyalty numbers and an ever-changing array of cookies picked up in browsers. The ID graph collects these identifiers and connects them to the customer's profile and any related data points, including behavioral data like browsing activity or purchase history."[55]

62. TikTok uses the information it collects through the TikTok Pixel to provide advertisers—like BCBS—with custom or lookalike audiences for purposes of targeted advertising campaigns.[56] TikTok can also sell the personal data it collects to data brokers and other third

[52] *Id.*

[53] *Id.*

[54] https://careers.tiktok.com/position/7132529118268442893/detail (emphasis added)

[55] https://signal.co/blog/6-things-about-id-graphs/

[56] https://ads.tiktok.com/help/article/ad-targeting?redirected=2

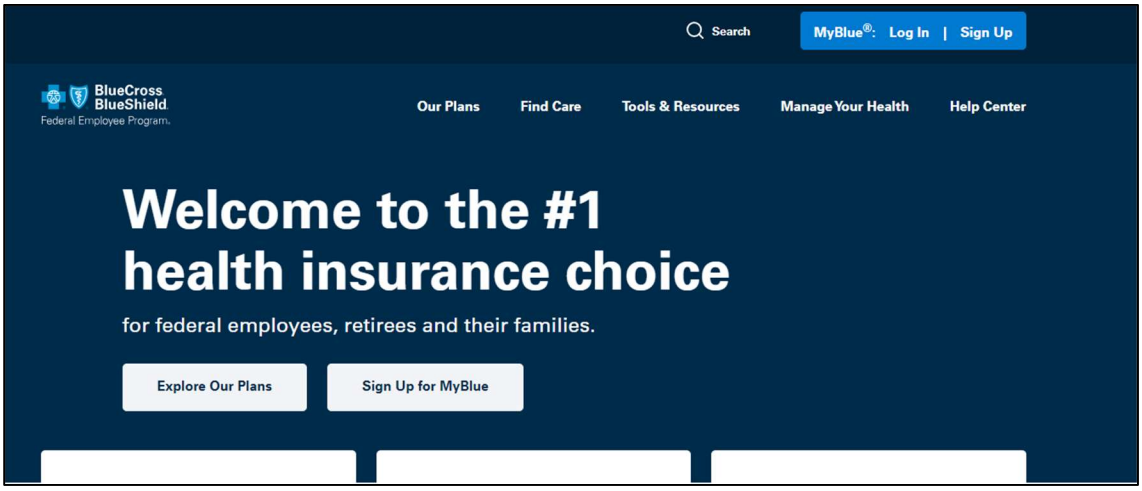
parties. Indeed, a recent analysis found that TikTok shared its users' data more than any other social media app, and it was unclear where the data went.[57]

D. Defendant Uses the TikTok Pixel to Intercept and Disclose Federal Employees' Sensitive Information to TikTok

63. Federal employees in the executive and judicial branches receive healthcare benefits through the Federal Employees Health Benefits ("FEHB") Program. The U.S. Office of Personnel Management ("OPM") administers the FEHB Program and contracts with private insurance companies to provide insurance plans consistent with the program's requirements.[58]

64. BCBS dominates the market under the FEHB Program, dwarfing other private insurance companies that contract with OPM. According to a study by the U.S. Government Accountability Office, "Blue Cross Blue Shield was the largest FEHB[] insurer in 93% of counties in 2000 and 98% of counties in 2015."[59]

65. The landing page for Defendant's Website confirms that it is "the # 1 health insurance choice for federal employees, retirees and their families," as reflected in ***Figure 1***:



[57] https://www.cnbc.com/2022/02/08/tiktok-shares-your-data-more-than-any-other-social-media-app-study.html

[58] https://www.opm.gov/healthcare-insurance/healthcare/

[59] https://www.gao.gov/products/gao-18-52

Figure 1: Landing Page of Defendants' Website

66. As the "#1 health insurance choice" for federal employees, BCBS was entrusted with protecting and safeguarding federal employees' Sensitive Information. Yet while federal and state governments across the county have banned TikTok on government devices, and national security experts have warned about TikTok's aggressive data-collection practices, Defendant has secretly deployed the TikTok Pixel on its Website to intercept the sensitive medical information of federal employees and transmit that information to TikTok.

67. Defendant's use of the TikTok Pixel on its Website—where federal employees can research specific symptoms and conditions, inquire about treatments, shop for insurance plans, and communicate other sensitive health-related information to their health insurer—is a flagrant breach of Defendant's duty to safeguard federal employees' Sensitive Information and constitutes a blatant violation of state and federal privacy laws.

68. Visitors to Defendants' Website can research symptoms, conditions, and treatments by navigating to designated subpages, as well as by typing information into the "search" bar on the Website. As a visitor navigates Defendant's Website, the visitor's browser sends HTTP requests to Defendant's webserver asking the server to display health-related information to the visitor. What the visitor does not know is that, with each communication from the visitor's browser to the Defendant's webserver, the TikTok Pixel simultaneously intercepts and duplicates the communication, redirecting it to TikTok's own servers.

69. As an example of how the TikTok Pixel operates on Defendant's Website, consider a federal employee who navigates to the "Manage Specific Conditions" subpage and selects "Mental Health." By clicking on "Mental Health," the employee's browser sends an HTTP request to Defendant's webserver to display the information on the "Mental Health" subpage.

Unbeknownst to the employee, that communication is also intercepted and re-directed to TikTok via the TikTok Pixel, as reflected in ***Figures 2*** and ***3***:

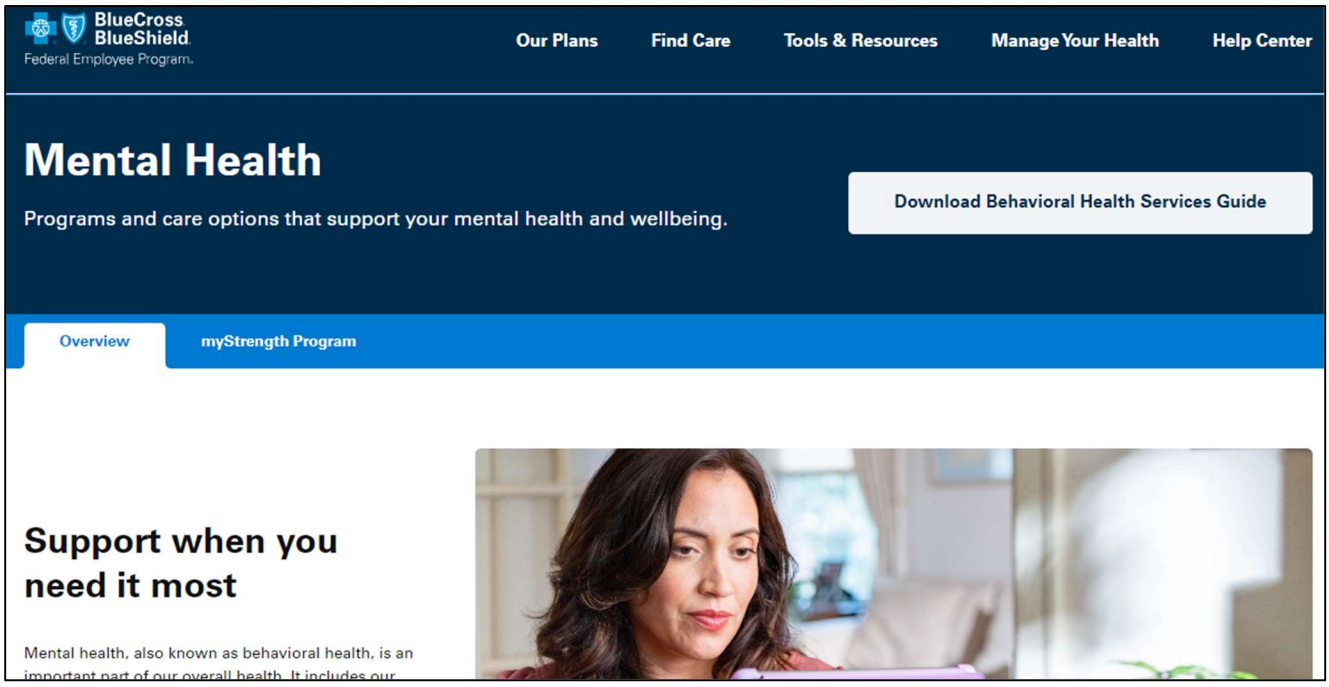


Figure 2: Display of "Mental Health" subpage

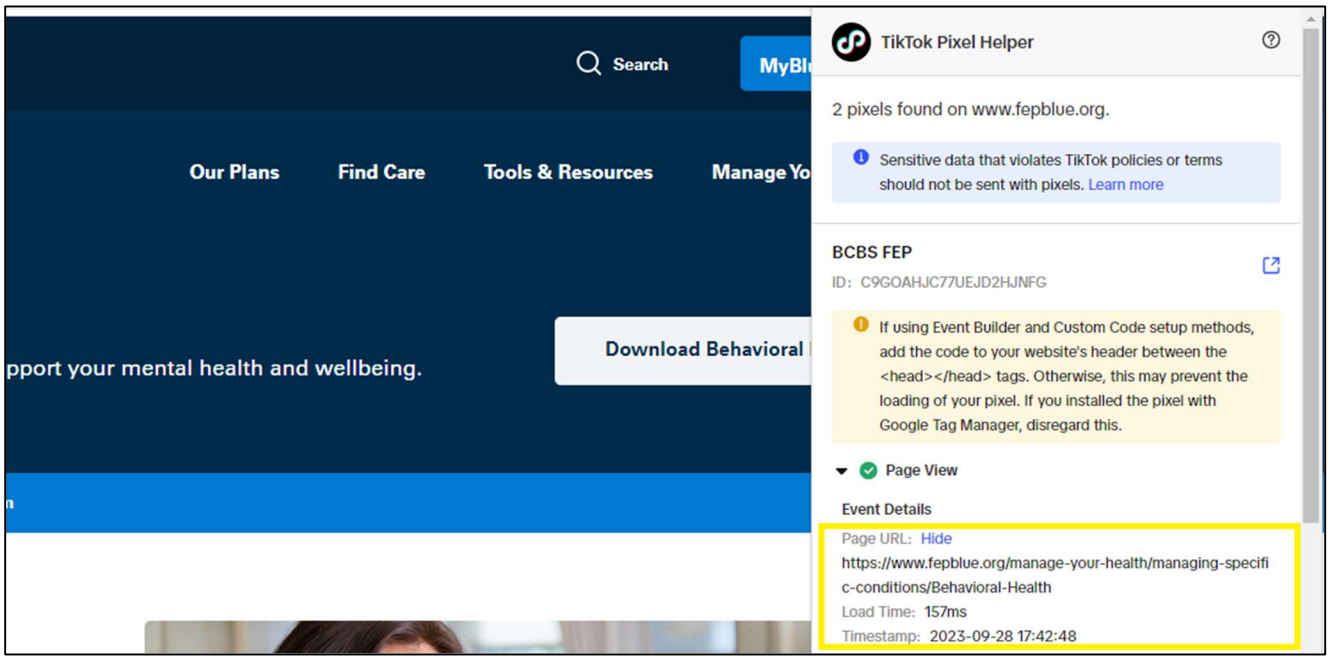


Figure 3: Display of content intercepted by TikTok

70. As reflected in ***Figure 3***, the TikTok Pixel intercepts and transmits to TikTok the URL information showing that the user was researching topics related to "Behavioral-Health," along with the specific date and time of the communication.

71. Similarly, instead of selecting "Mental Health," on the "Manage Specific Conditions" subpage, if the federal employee clicked on "Pregnancy," the employee's browser would send an HTTP request to Defendant's webserver to display the page shown in ***Figure 4***:

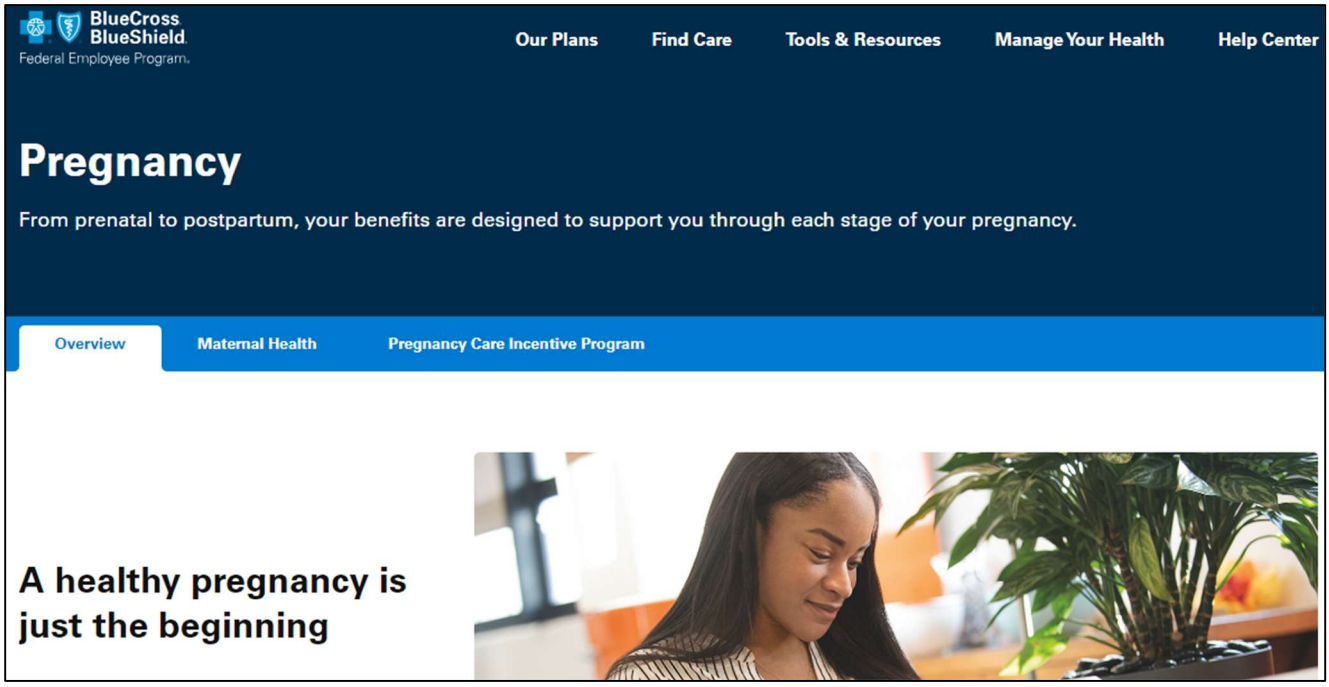


Figure 4: Display of "Pregnancy" subpage

72. Because Defendant deploys the TikTok Pixel on its Website, the federal employee's online communication is simultaneously intercepted and re-directed to TikTok, as shown in ***Figure 5***:

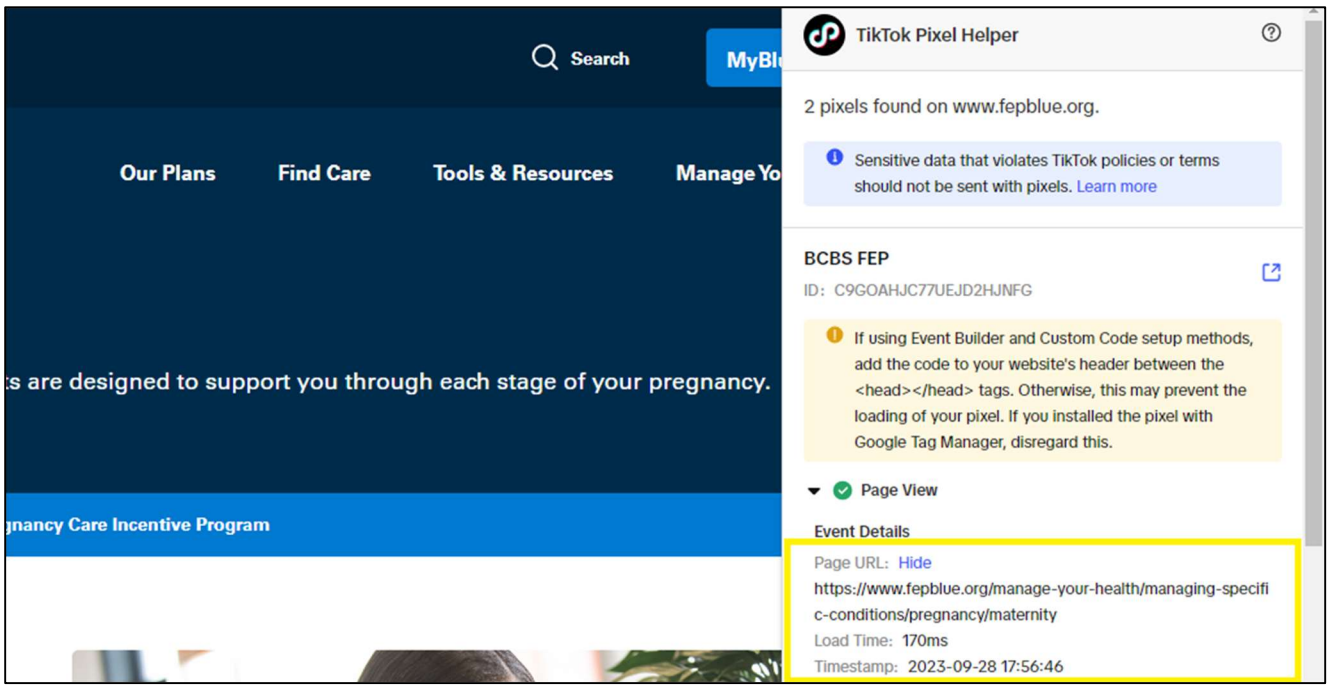


Figure 5: Display of content intercepted by TikTok

73. As another example, rather than navigating to the "Manage Specific Conditions" page, if a federal employee instead typed words into the Website's "search" bar regarding sensitive health-related topics, such as "addiction" or "depression," the employee's browser would send an HTTP request to Defendant's webserver to display the following information about those topics, and the employee's communications would be intercepted and redirected to TikTok, as shown in ***Figures 6*** and ***7***:

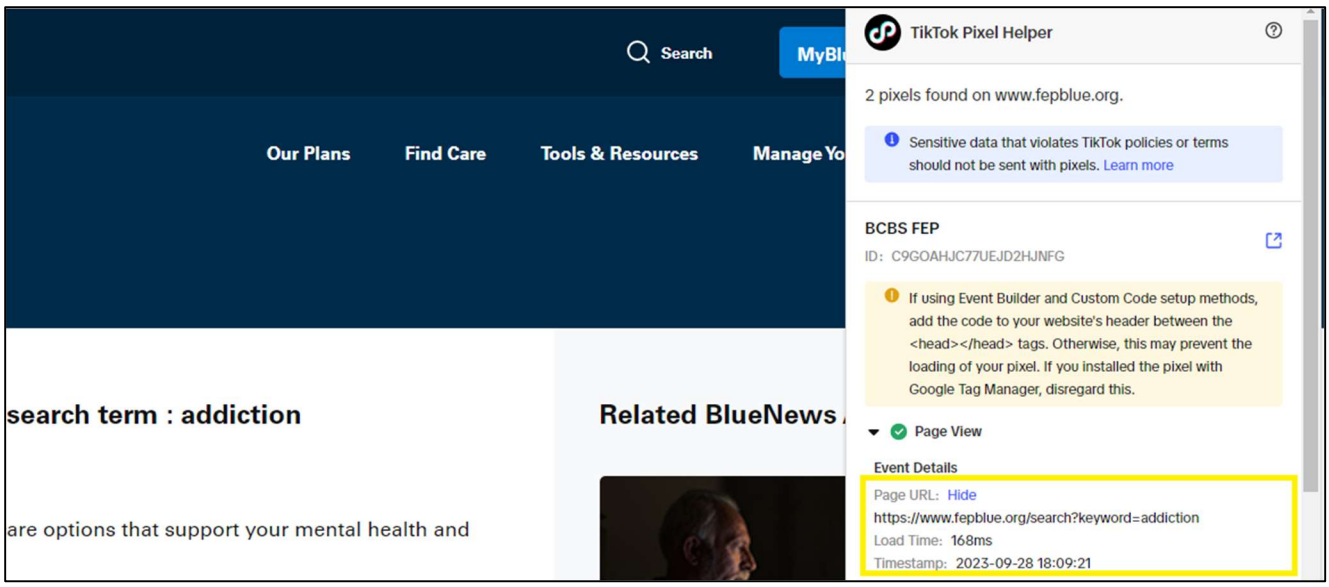


Figure 6: Display of "addiction" query intercepted by TikTok

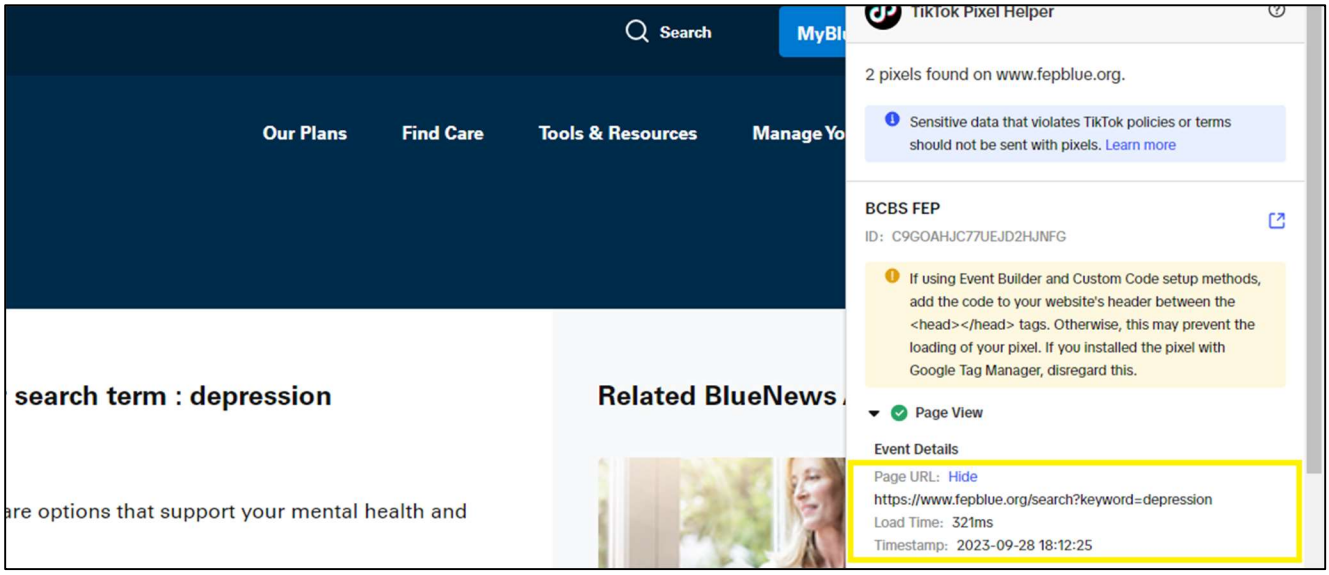


Figure 7: Display of "depression" query intercepted by TikTok

74. A federal employee who shops for different health plans on Defendant's Website is also subject to TikTok's illegal surveillance. If an employee selected the "FEP Blue Focus," plan, for example, the lowest-cost plan that is supposed to be "easy on your wallet," the employee's communications with Defendant would result in the following page being displayed, and TikTok would also receive the same information via the TikTok Pixel, as shown in ***Figure 8***:

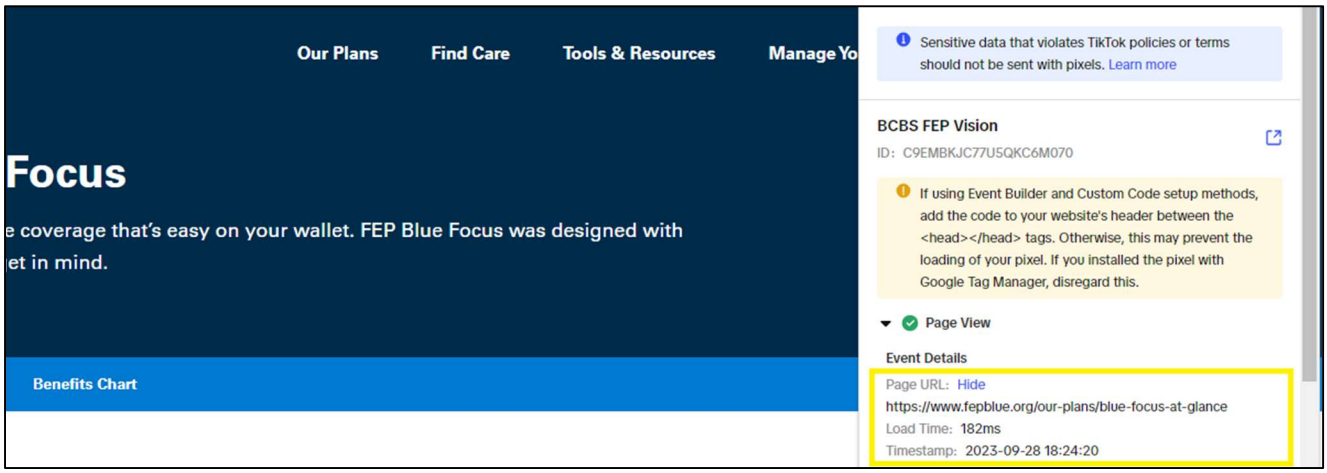


Figure 8: Display of "FEP Blue Focus" plan information intercepted by TikTok

75. If the federal employee had a TikTok account, each online communication with Defendant (as reflected in the above examples) would be transmitted to TikTok along with unique identifiers that TikTok could use to match the communications with a TikTok account and identified user.

76. Based on that information, TikTok would know the exact day and time that an identified federal employee researched specific health-related topics, including particular symptoms and conditions such as "Mental Health," "Pregnancy," and "addiction."

77. Even if the employee did not have a TikTok account, the TikTok Pixel would transmit the employee's communications to TikTok with cookies and other unique identifiers that make up the employee's "fingerprints,"—including, for example, the employee's IP address and

identifiers associated with the employee's browser and device—which TikTok could combine with other data harvested from the internet at large in an effort to identify the employee through a robust identity graph.

78. Once TikTok had that information, it could use it for any purpose, and the federal employee would have no way of deleting or retrieving the sensitive data.

E. Defendant's Disclosure of Federal Employees' Sensitive Information to TikTok Raises Serious Privacy and National Security Concerns

79. The U.S. Government has taken swift and decisive steps to mitigate the privacy and security concerns related to TikTok's data-harvesting campaign, including banning the use of TikTok on official devices and systems for members of Congress, members of the executive branch, and federal contractors.

80. These preventative actions arose out of widespread bipartisan concerns over TikTok's close ties to China and the serious risk that the massive amounts of personal data TikTok collected would end up in the hands of the Chinese government. Referring to the White House's February 2023 announcement banning TikTok on government devices, the Office of Management and Budget stated, "[this is a] critical step forward in addressing the risks presented by the app to sensitive government data."[60]

81. Those risks include the threat of blackmail or extortion of federal employees in sensitive positions. An August 2020 Executive Order from the White House declared that TikTok's "data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information — potentially allowing China to track the locations of

[60] https://apnews.com/article/technology-politics-united-states-government-ap-top-news-business-95491774cf8f0fe3e2b9634658a22e56

Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."[61]

82. National security and cybersecurity experts have echoed the same concerns.[62] A computer scientist at Vanderbilt University described how this could play out: "If you're a government employee, and somebody can figure out you have access to some sensitive information or some sensitive budget things, and they can get blackmail information because they know what websites you look at or who you talk to . . . [y]ou can imagine people being more susceptible in those situations."[63] A professor at Cornell University similarly commented that, through TikTok's data-collection practices, "China could conduct surveillance on specific users, [or] collect compromising, blackmail-worthy information."[64]

83. Defendant's disclosure of federal employees' sensitive medical information to TikTok exacerbates those concerns. While the U.S. government has taken steps to protect against the risks of TikTok's collection of federal employees' personal data, Defendant has secretly left the back door wide open, allowing TikTok to gather sensitive medical information related to employees' specific symptoms and conditions. In doing so, Defendant subjected federal employees to the loss of their sensitive medical data and to the risk of blackmail and extortion by a foreign power.

[61] https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/

[62] https://apnews.com/article/technology-china-united-states-national-security-government-and-politics-ac5c29cafaa1fc6bee990ed7e1fe5afc

[63] https://newjerseymonitor.com/2022/12/21/tiktok-ban-for-federal-workers-close-to-becoming-law-following-flurry-of-state-bans/

[64] https://news.cornell.edu/media-relations/tip-sheets/tiktok-ban-reasonable-given-threat-chinese-surveillance

84. To compound the harm, federal employees' sensitive medical information harvested via the TikTok Pixel can potentially be combined with massive amounts of personal data exfiltrated by China-based actors in connection with the 2015 hack on OPM systems (which breached millions of federal employees' background security checks), as well as other hacking operations originating from China. As one commentator highlighted:

> By combining personnel data with travel records, health records, and credit information, Chinese intelligence has amassed in just five years a database more detailed than any nation has ever possessed about one of its adversaries. The data and its layers work both to identify existing US intelligence officers through their personnel records and travel patterns as well as to identify potential weaknesses—through background checks, credit scores, and health records—of intelligence targets China may someday hope to recruit.[65]

F. Defendant Uses Other Tracking Technologies that Disclose Federal Employees' Sensitive Information to Meta, Google, and LinkedIn

85. In addition to its use of the TikTok Pixel, Defendant's Website uses tracking technologies from at least three other companies that result in the unauthorized disclosure of federal employees' Sensitive Information. The tracking technologies include: (1) the Meta Pixel, (2) Google Analytics, and (3) the LinkedIn Insight Tag.

86. These three tracking technologies work in substantially the same manner as the TikTok Pixel. They all intercept and redirect the website user's communications with Defendant's Website—including specific URL information showing the pages visited, buttons clicked, and search queries conducted by visitors—to unauthorized third parties. On information and belief, Meta, Google, and LinkedIn then match the communications with account holders for purposes of targeted advertising or otherwise monetizing the user data. While the disclosures to Meta, Google, and LinkedIn do not necessarily raise the same national security concerns as the disclosures to

[65] https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/

TikTok, they nonetheless constitute violations of federal employees' privacy rights under state and federal law.

i. Meta Pixel

87. Like the TikTok Pixel, the Meta Pixel is a piece of code that website developers can incorporate into their websites to track user activities. The Meta Pixel records a user's IP address, pages viewed (such as specific URL information), buttons clicked, search queries, and other user activities on a website. Like TikTok, Meta is able to link a user's online communications to a specific Facebook account holder through cookies and other unique identifiers.

88. Meta does this by placing cookies in the web browsers of users logged into their services. The "c_user" cookie, for example, contains a numerical value known as the Facebook ID, which uniquely identifies a Facebook user. When a Facebook user visits the Defendant's Website while logged-in to their Facebook account, the Meta Pixel transmits the user's private web communications with the Defendant along with the "c_user" cookie. Meta can then use this information to match the web communications with the user's Facebook ID.

89. Even if a user does not have a Facebook account or is not logged-in to Facebook when browsing the Defendant's Website, the Meta Pixel transmits the user's web communications with Defendant's Website to Meta along with a unique identifier associated with another cookie called the "_fbp" cookie. Meta can then use that unique identifier, along with other persistent cookies, to link the user's web communications with the user's Facebook ID. And if a user who does not have a Facebook account later creates an account, Meta may be able to associate the user's historical browsing history intercepted via the Pixel and "_fbp" cookie to the newly created account.

90. As an example of how the Meta Pixel operates on Defendant's website, consider a federal employee who navigates to the "Coronavirus Resource Center" page. To access that page, the employee's browser would send a GET request to Defendant's webserver to display the page shown in ***Figure 9***:

Figure 9: Display of "Coronavirus Resource Page"

91. Because Defendant deploys the Meta Pixel on its Website, the communication from the employee's browser to Defendant's webserver would be intercepted and transmitted to Meta along with unique identifiers, such as the c_user and _fbp cookies, which Meta could use to match the communication to a Facebook account, as shown in ***Figure 10***:

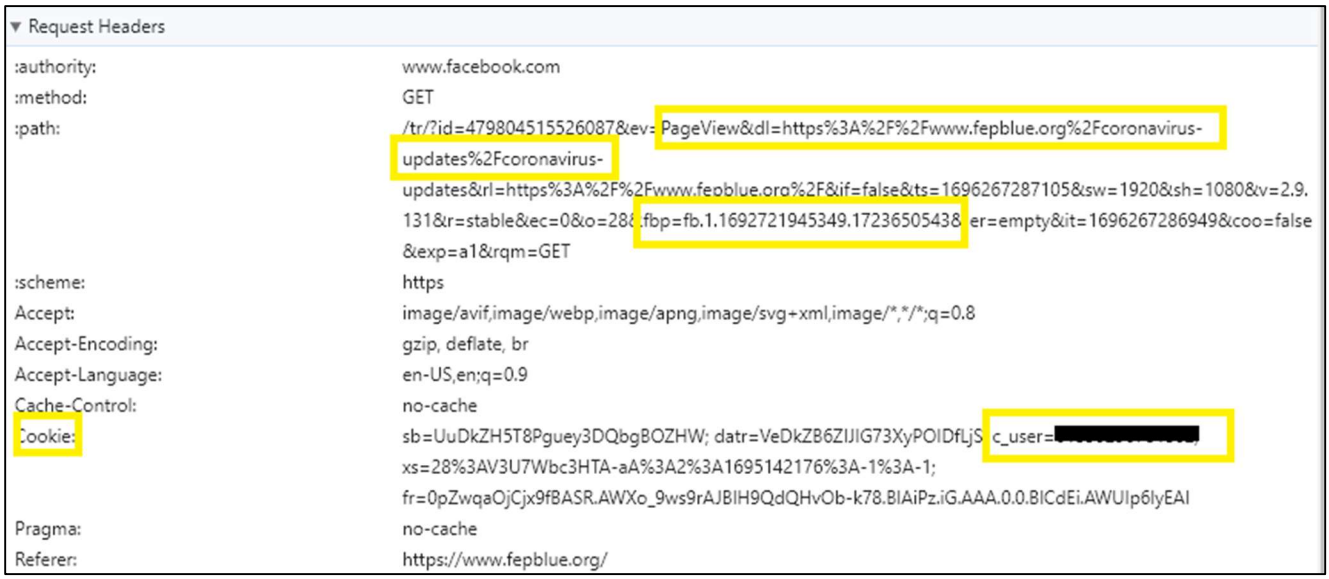


Figure 10: Display of information intercepted by Meta

92. As shown in ***Figure 10***, the specific URL information revealing the substance of the employee's communication ("coronavirus updates") is intercepted and transmitted to Meta along with the cookies used to match the communication to a Facebook account.

ii. Google Analytics

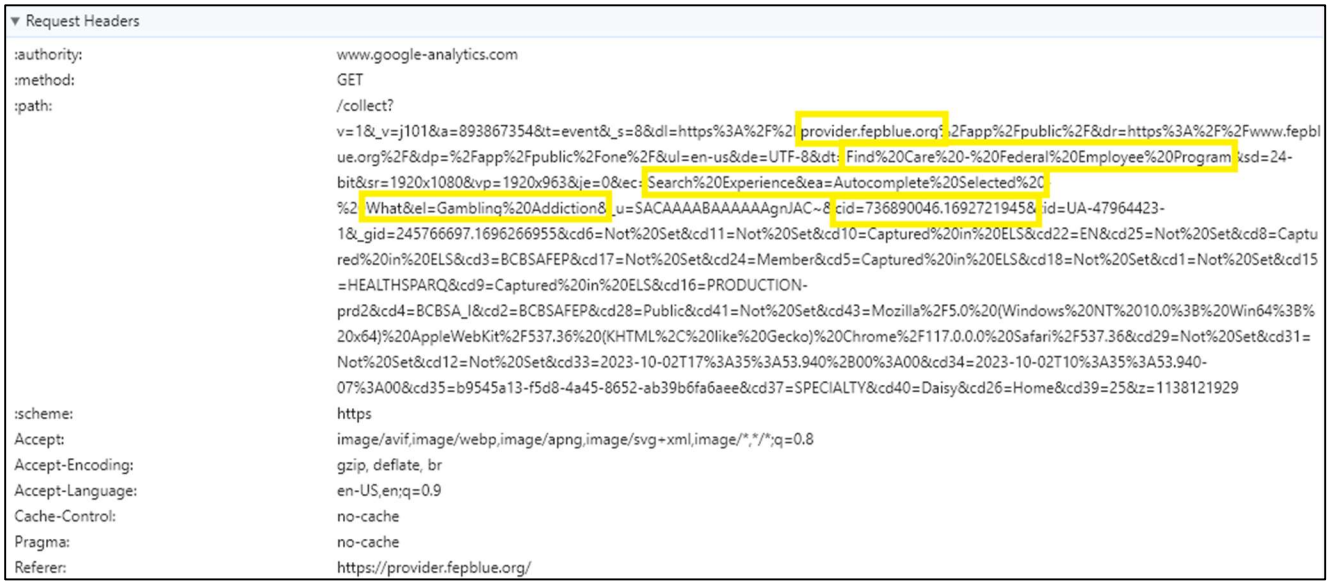
93. Like the TikTok Pixel and the Meta Pixel, Google Analytics consists of code that website developers can install on their websites to track user activity. Whenever a user visits a website that is running Google Analytics, Google's code directs the user's browser to send a separate and concurrent communication to Google without the user's knowledge.

94. The information that is intercepted and transmitted to Google via the Google Analytics code includes: the URL of the specific webpage the user is trying to access; the user's IP address; the User-agent, which identifies the user's device platform and browser; the user's geolocation, if available; the Referer, which is the URL of the page on which the user clicked a link to access a new page; event data, which describes how users interact with a website, for

example, whether they saw an ad or played a video; and the actual search queries on the site. In this way, Google Analytics tells Google exactly what a user's browser communicated to the website.

95. Like the TikTok Pixel and the Meta Pixel, the user's communications to the website are transmitted to Google together with cookies and other unique identifiers that Google can use to match the communications to individuals who use Google's services.

96. As an example of how Google Analytics operates on Defendant's website, consider a federal employee who searches for a doctor by specialty and selects "Gambling addiction." By making that selection, the employee's browser sends a GET request to Defendant's webserver to display a list of providers who specialize in "Gambling addiction." At the same time, Google's code causes the employee's browser to send the same communication to Google, as shown in ***Figure 11***:



▼ Request Headers

:authority:	www.google-analytics.com
:method:	GET
:path:	/collect? v=1&_v=j101&a=893867354&t=event&_s=8&dl=https%3A%2F%2[provider.fepblue.org[2Fapp%2Fpublic%2F&dr=https%3A%2F%2Fwww.fepbl ue.org%2F&dp=%2Fapp%2Fpublic%2Fone%2F&ul=en-us&de=UTF-8&dt= Find%20Care%20-%20Federal%20Employee%20Program &sd=24- bit&sr=1920x1080&vp=1920x963&je=0&ec= Search%20Experience&ea=Autocomplete%20Selected%20 %2 What&el=Gambling%20Addiction& _u=SACAAAABAAAAAAgnJAC~8 cid=736890046.16927219458 id=UA-47964423- 1&_gid=245766697.1696266955&cd6=Not%20Set&cd11=Not%20Set&cd10=Captured%20in%20ELS&cd22=EN&cd25=Not%20Set&cd8=Captu red%20in%20ELS&cd3=BCBSAFEP&cd17=Not%20Set&cd24=Member&cd5=Captured%20in%20ELS&cd18=Not%20Set&cd1=Not%20Set&cd15 =HEALTHSPARQ&cd9=Captured%20in%20ELS&cd16=PRODUCTION- prd2&cd4=BCBSA_I&cd2=BCBSAFEP&cd28=Public&cd41=Not%20Set&cd43=Mozilla%2F5.0%20(Windows%20NT%2010.0%3B%20Win64%3B% 20x64)%20AppleWebKit%2F537.36%20(KHTML%2C%20like%20Gecko)%20Chrome%2F117.0.0.0%20Safari%2F537.36&cd29=Not%20Set&cd31= Not%20Set&cd12=Not%20Set&cd33=2023-10-02T17%3A35%3A53.940%2B00%3A00&cd34=2023-10-02T10%3A35%3A53.940- 07%3A00&cd35=b9545a13-f5d8-4a45-8652-ab39b6fa6aee&cd37=SPECIALTY&cd40=Daisy&cd26=Home&cd39=25&z=1138121929
:scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:	gzip, deflate, br
Accept-Language:	en-US,en;q=0.9
Cache-Control:	no-cache
Pragma:	no-cache
Referer:	https://provider.fepblue.org/

Figure 11: Information intercepted by Google

iii. LinkedIn Insight Tag

97. LinkedIn is the largest social media platform geared specifically to professionals. LinkedIn boasts a membership of approximately 980 million users in more than 200 countries and territories worldwide. Like other social media companies, LinkedIn generates substantial revenue through its advertising program, bringing in more than $3 billion in revenue in 2021. For companies looking to advertise, LinkedIn pitches its ability to "[r]each the right audience," through "[p]recise and powerful audience targeting."[66] This allows companies and advertisers to "[t]arget [their] ideal customer based on traits like their job title, company name or industry, and by professional or personal interests."[67]

98. LinkedIn's ability to provide advertisers with precise target audiences comes from information users provide to LinkedIn as well as information LinkedIn learns about its users using online tracking technology.

99. One of LinkedIn's online tracking tools is the LinkedIn Insight Tag. According to LinkedIn, "[t]he LinkedIn Insight Tag is a piece of lightweight JavaScript code that [companies] can add to [their] website to enable in-depth campaign reporting and unlock valuable insights about [their] website visitors."[68] The LinkedIn Insight Tag "enables the collection of data regarding members' visits to [a] website, including the URL, referrer, IP address, device and browser characteristics (User Agent), and timestamp."[69]

---

[66] https://business.linkedin.com/marketing-solutions/ad-targeting

[67] *Id.*

[68] https://www.linkedin.com/help/lms/answer/a427660

[69] What data does my website send through this tag and how is it used? https://www.linkedin.com/help/lms/answer/a427660

100. The LinkedIn Insight Tag also transmits various cookies and unique identifiers to LinkedIn that allow LinkedIn to match the user's activity on the website to the user's LinkedIn account. And if the user does not have a LinkedIn account, the data still includes unique identifiers, such as the user's IP address and device and browser characteristics.[70]

101. As an example of how the LinkedIn Insight Tag operates on Defendant's website, consider a federal employee who types "cancer coverage" into the Website's search bar. By typing that information into the search bar, the employee's browser transmits a GET request to the Defendant's webserver to display information about "cancer coverage," and the LinkedIn Insight Tag causes the browser to transmit the same information to LinkedIn along with various cookies that LinkedIn can use to match the communication to an identified user, as shown in ***Figure 12***:

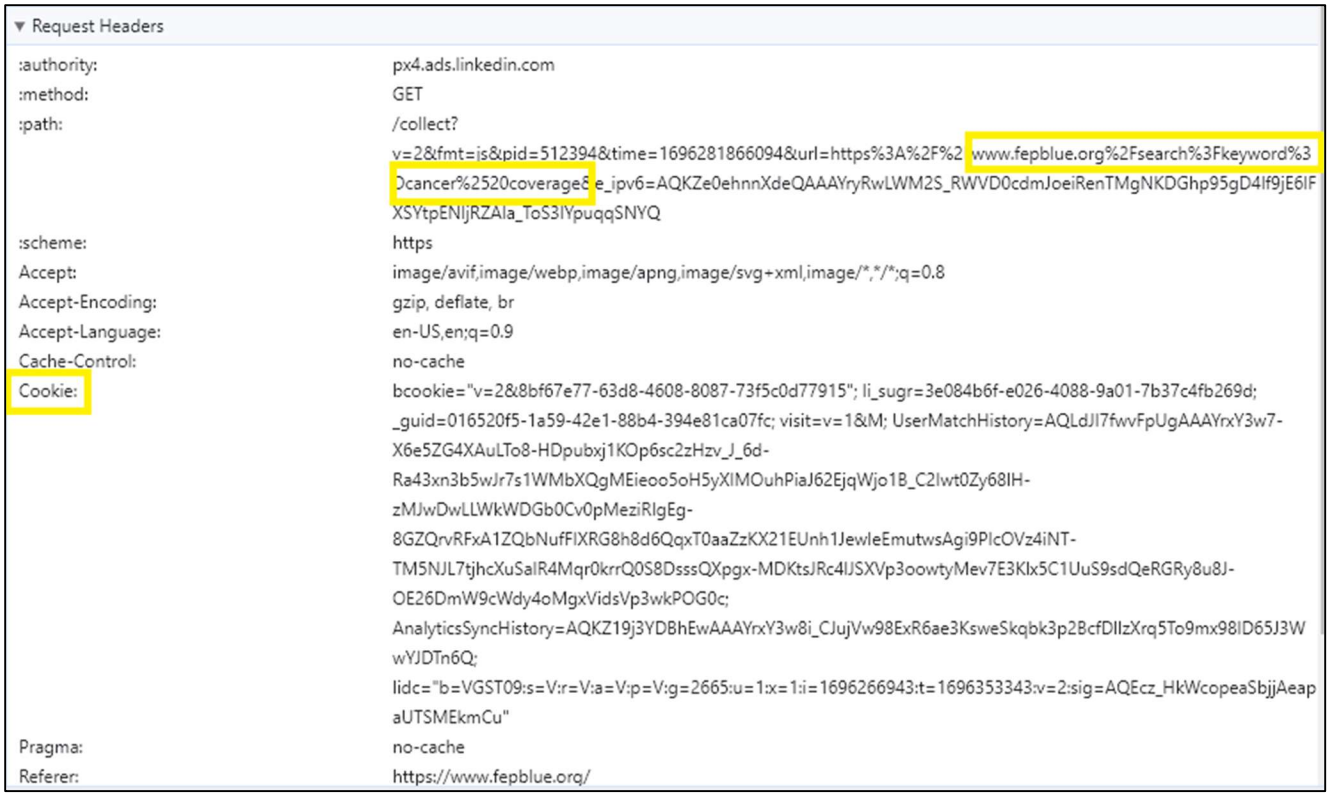


Figure 12: Information intercepted by LinkedIn

[70] *See id.*

102. By disclosing federal employees' Sensitive Information to third-party technology companies—including TikTok, Meta, Google, and LinkedIn—without the employees' knowledge or consent, Defendant breached its duty to safeguard medical information against unauthorized dissemination and violated employees' privacy rights under state and federal law.

G. Exposure of Sensitive Information Creates a Substantial Risk of Harm

103. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[71]

104. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require, among other things: (1) using industry tested and accepted methods; (2) monitoring activity on networks to uncover unapproved activity; (3) verifying that privacy and security features function properly; and (4) testing for common vulnerabilities or unauthorized disclosures.[72]

105. The FTC cautions businesses that failure to protect Sensitive Information and the resulting privacy breaches can destroy consumers' finances, credit history, and reputations, and can take time, money and patience to resolve the effect.[73] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures as an unfair act or practice prohibited

[71] https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

[72] https://www.ftc.gov/business-guidance/resources/start-security-guide-business

[73] https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf

by Section 5(a) of the FTC Act. These harms are in addition to the serious privacy and national security threats posed by the disclosure of federal employees' Sensitive Information to TikTok specifically.

H. Plaintiffs' and the Class's Sensitive Information is Valuable

106. The personal and health information of Plaintiffs and the Class is valuable and has become a highly desirable commodity. Indeed, one of the world's most valuable resources is the exchange of personal data.[74]

107. Business News Daily reported that businesses collect personal data (i.e., gender, web browser cookies, IP addresses, and device IDs), engagement data (i.e., consumer interaction with a business's website, applications, and emails), behavioral data (i.e., customers' purchase histories and product usage information), and attitudinal data (i.e., consumer satisfaction data) from consumers.[75] Companies then use this data to impact the customer experiences, modify their marketing strategies, publicly disclose or sell data, and even to obtain more sensitive data that may be even more lucrative.[76]

108. The power to capture and use customer data to manipulate products, solutions, and the buying experience is invaluable to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[77]

---

[74]https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[75] https://www.businessnewsdaily.com/10625-businesses-collecting-data.html

[76] *Id.*

[77]https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data

109. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[78] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[79]

110. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[80]

111. Unlike financial information, such as credit card and bank account numbers, PHI and certain PII cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or her life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable.[81]

112. Consumers place a considerable value on their Sensitive Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between $30.49

[78] https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf

[79] *Id.* at 25.

[80] *Id.*

[81] https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/

and $44.62.[82] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

113. Defendant's privacy violations exposed a variety of Sensitive Information, including medical conditions, symptoms, treatments sought, physicians, search queries, and other highly sensitive data.

114. Some industry insiders and journalists are even calling hospitals the "brokers to technology companies" for their role in data sharing in the $3 trillion healthcare sector.[83] "Rapid digitization of health records … have positioned hospitals as a primary arbiter of how much sensitive data is shared."[84]

115. Third-party technology companies, like TikTok, Meta, Google, and LinkedIn, generate a substantial portion of their revenue through highly targeted advertising—a valuable service that is enabled by entities like Defendant sharing information about their users' online activities. Entities, like Defendant, likewise benefit financially from the collection and sharing of user data by increasing sales or customer acquisitions while also reducing advertising costs.[85] Through Defendant's conduct described herein, Plaintiffs and the Class lost the benefit and financial value of their private data, while Defendant unjustly benefitted.

I. Plaintiffs and the Class Had a Reasonable Expectation of Privacy in Their Interaction with Defendant's Website

116. Consumers are concerned about entities, like Defendant, collecting their data and assume the data they provide, particularly highly sensitive medical data, will be kept secure and

[82] https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf

[83] https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200

[84] *Id.*

[85] https://www.facebook.com/business/tools/meta-pixel/case-studies

private.

117. In a recent survey related to internet user expectations, most website visitors indicated they assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.[86] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[87]

118. The majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its' customers' data.[88] A March 2000 BusinessWeek/Harris Poll found that 89% of respondents were uncomfortable with web tracking schemes where data was combined with an individual's identity.[89] The same poll found that 63% of respondents were uncomfortable with web tracking even where the clickstream data was not linked to personally identifiable information.[90] A July 2000 USA Weekend Poll showed that 65% of respondents thought that tracking computer use was an invasion of privacy.[91]

119. Patients and website users act consistently with their expectation of privacy. For example, following a new rollout of iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and

[86] https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html

[87] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, THE INFORMATION SOCIETY, 38:4, 257, 258 (2022).

[88] https://archive.epic.org/privacy/survey/

[89] *Id.*

[90] *Id.*

[91] *Id.*

94 percent of U.S. users chose not to allow such tracking.[92]

120. Like the greater population, Defendant's patients and prospective patients would expect the highly sensitive *medical* information they provided to Defendant through its Website to be kept secure and private.

121. Further, given the U.S. government's swift and decisive actions to prevent the disclosure of sensitive government information to TikTok and avoid the risks of blackmail or extortion, federal employees would reasonably expect that the largest health insurance contractor under the FEHB program would not disclose sensitive medical information to TikTok.

J. Defendant's Conduct Violated HIPAA

122. Under HIPAA, individuals' health information must be:

> properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.[93]

123. HIPAA is a "federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[94] The rule requires appropriate administrative, physical, and technological safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.[95]

124. The Privacy Rule protects from unauthorized disclosure all "individually identifiable health information" held or transmitted by a covered entity or its business associate,

---

[92] https://www.wired.co.uk/article/apple-ios14-facebook

[93] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[94]https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=Health%20Insurance%20Portability%20and%20Accountability%20Act%20of%201996%20(HIPAA),-On%20This%20Page&text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge

[95] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)." "Individually identifiable health information" is information, (1) that relates to: the individual's past, present or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual; and (2) that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.[96]

125. The U.S. Department of Health and Human Services, Office for Civil Rights ("OCR") issued guidance in December 2022 warning about violations of the Privacy Rule based on the use of tracking technologies on health-care providers' websites. According to the OCR guidance, "Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."[97] This includes "disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations."[98]

126. OCR specifically warned about the dangers of disclosing PHI through a website's "unauthenticated webpage," or the portion of the site that does "not require users to log in before they are able to access the webpage."[99] According to the OCR guidance, "in some cases, tracking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to the tracking technology vendors."[100] Examples include, "[t]racking technologies on a regulated entity's

---

[96] *Id.*

[97] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html#ftnref29

[98] *Id.*

[99] *Id.*

[100] *Id.*

unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials," and that are tied to individual identifiers, such as "an individual's email address and/or IP address."[101]

127. Finally, the OCR guidance explained that data that could be used to identify individuals—such as IP addresses—qualified as PHI even if the person did not have an existing relationship with the health care provider. According to the OCR guidance, information gathered through tracking technologies on healthcare websites,

> might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.[102]

128. BCBS is a covered entity for purposes of HIPAA and the Privacy Rule.[103] Through its use of tracking technologies on its Website to intercept and transmit Sensitive Information about

[101] *Id.*; *see also* 45 C.F.R. § 164.514 (2) (defining personally identifiable information to include "any unique identifying number, characteristic or code" and specifically listing the example of IP addresses).

[102] *Id.*

[103] https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html#:~:text=We%20call%20the%20entities%20that,such%20as%20Medicare%20and%20Medicaid. (noting that covered entities include "Health Plans, including health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid").

federal employees—along with identifiers (such as IP addresses and cookies) that third-party technology companies can use to identify the federal employees—Defendant violated HIPAA.

129. Further, Defendant made these unauthorized disclosures without obtaining HIPAA-compliant consent from Plaintiffs and the Class. Under 45 C.F.R. § 164.508(c)(1), for a HIPAA authorization of disclosure to be valid, it must:

a. Describe the specific PHI the patient is authorizing be shared;

b. Name the entities authorized to make the disclosure;

c. Name the persons or entities to whom disclosure may be made;

d. Describe the purpose of the requested use or disclosure;

e. Contain an expiration date; and

f. Contain a signature and date.

130. Defendant did not obtain HIPAA-compliant authorization from Plaintiffs and the Class. Defendant did not, for example, disclose to federal employees that it allows TikTok to intercept and record their communications to Defendant via the Website, including communications about sensitive medical information. Nor did Defendant obtain Plaintiffs' and the Class's signatures to disclose their sensitive PHI to other third-party technology companies.

CLASS PERIOD

131. For purposes of this Class Action Complaint, the Class Period corresponds to the period between November 2021 and the present and runs until such date as the Court enters an Order certifying any Count of this Class Action Complaint for class action treatment.

CLASS ALLEGATIONS

132. Plaintiffs bring this class action pursuant to Fed. R. Civ. P. 23 on behalf of themselves and all others similarly situated, as representatives of the following Classes:

Nationwide class

All persons participating in the FEHB program whose Sensitive Information was disclosed to a third-party through Defendant's Website without authorization or consent during the Class Period.

California class

All residents of California participating in the FEHB program whose Sensitive Information was disclosed to a third-party through Defendant's Website without authorization or consent during the Class Period.

133. Excluded from the Classes are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest in, is a parent or subsidiary of, or which is otherwise controlled by Defendant; and Defendant's affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assignees. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

134. Plaintiffs reserve the right to modify and/or amend the Class definitions as necessary.

135. All members of the proposed Classes are readily identifiable through Defendant's records.

136. All requirements for class certification under Fed. R. Civ. P. 23(a), 23(b)(2) and 23(b)(3) are satisfied.

137. **Numerosity.** The members of the Classes are so numerous that joinder of all members of the Classes is impracticable. Plaintiffs are informed and believe that the proposed Classes includes over one million people. The precise number of Class Members is unknown to Plaintiffs but may be ascertained from Defendant's records.

138. **Commonality and Predominance.** This action involves common questions of law and fact to the Plaintiffs and Class Members, which predominate over any questions only affecting

individual Class Members. These common legal and factual questions include, without limitation:

a. Whether Plaintiffs' and Class Members' communications with Defendant's Website were unlawfully intercepted and disclosed to third parties;

b. Whether Defendant made use of and derived a benefit from the intercepted communications;

c. Whether the interception and disclosure of Plaintiffs' and Class Members' communications were consensual;

d. Whether Defendant owed Plaintiffs and the other Class Members a duty to adequately protect their Sensitive Information;

e. Whether Defendant owed Plaintiffs and the other Class Members a duty to secure their Sensitive Information from disclosure via third-party tracking technologies;

f. Whether Defendant owed Plaintiffs and the other Class Members a duty to implement reasonable data privacy protection measures because Defendant accepted, stored, created, and maintained highly sensitive information concerning Plaintiffs and the Class;

g. Whether Defendant knew or should have known of the risk of disclosure of data through third-party tracking technologies;

h. Whether Defendant breached its duty to protect the Sensitive Information of Plaintiffs and other Class Members;

i. Whether Defendant knew or should have known about the inadequacies of its privacy protection;

j. Whether Defendant failed to use reasonable care and reasonable methods to safeguard and protect Plaintiffs' and the Class's Sensitive Information from unauthorized disclosure;

k. Whether proper data security measures, policies, procedures and protocols were enacted within Defendant's computer systems to safeguard and protect Plaintiffs' and the Class's Sensitive Information from unauthorized disclosure;

l. Whether Defendant's conduct was the proximate cause of Plaintiffs' and the Class's injuries;

m. Whether Plaintiffs and the Class had a reasonable expectation of privacy in their Sensitive Information;

n. Whether Plaintiffs and the Class suffered ascertainable and cognizable injuries as a result of Defendants' misconduct;

o. Whether Plaintiffs and the Class are entitled to recover damages; and

p. Whether Plaintiffs and the Class are entitled to other appropriate remedies including injunctive relief.

139. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiffs on behalf of themselves and the Classes. Individual questions, if any, are slight by comparison in both quality and quantity to the common questions that control this action.

140. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Sensitive Information, like that of every other Class member, was improperly disclosed by Defendant. Defendant's misconduct impacted all Class Members in a similar manner.

141. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interest of the members of the Classes and have retained counsel experienced in complex consumer class

action litigation and intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Classes.

142. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class Members in a single action will provide substantial benefits to all parties and to the Court. Absent a class action, individual patients like Plaintiffs would find the cost of litigating their claims prohibitively high and would have no effective remedy for monetary relief.

143. Class Certification under Fed. R. Civ. P. 23(b)(2) is also appropriate. Defendant has acted or refused to act on grounds that apply generally to the Classes, thereby making monetary, injunctive, equitable, declaratory, or a combination of such relief appropriate. As Defendant continues to engage in the practices described herein, the risk of future harm to Plaintiffs and the Classes remains, making injunctive relief appropriate. The prosecution of separate actions by all affected individuals with dealings similar to Plaintiffs', even if possible, would create a substantial risk of (a) inconsistent or varying adjudications with respect to individual employees, which would establish potentially incompatible standards of conduct for Defendant, and/or (b) adjudications with respect to individual employees which would, as a practical matter, be dispositive of the interests of the other employees not parties to the adjudications, or which would substantially impair or impede the ability to protect the interests of the Classes. Further, the claims

of individual employees in the defined Classes are not sufficiently large to warrant vigorous individual prosecution considering all of the concomitant costs and expenses.

CLAIMS

COUNT I
VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA") 18 U.S.C. § 2511(1), *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class)

144. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

145. The primary purpose of ECPA is to protect the privacy of communications.

146. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of ECPA.

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

148. Content. ECPA defines content, when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). Plaintiffs' and Class Members' Sensitive Information—including information about symptoms, conditions, treatments, and other health-related queries as revealed by full-string URL's—constitute "content" under ECPA.

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

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

151. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's web-servers; and,

d. The tracking technology code deployed by Defendant to effectuate the interception of Plaintiffs' and Class Members' communications.

152. By utilizing and embedding the tracking technologies from TikTok, Meta, Google, and LinkedIn on its Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

153. The intercepted content included, but was not limited to, communications from Plaintiffs and Class Members regarding Sensitive Information, such as symptoms, conditions, and treatments.

154. By intentionally disclosing or endeavoring to disclose Plaintiffs' and Class Members' electronic communications to third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

155. By intentionally using, or endeavoring to use, the contents of Plaintiffs' and Class Members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of

18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d). Specifically, Defendant intentionally used the unlawfully intercepted content for its own marketing, advertising, and analytics purposes.

156. Unauthorized Purpose. The contents of Plaintiffs' and Class Members' electronic communications were intentionally intercepted for the purpose of committing tortious and criminal acts in violation of the Constitution or laws of the United States or of any State. Indeed, Defendant's primary purpose for deploying the tracking technologies was to collect data from users secretly, deceptively, and without permission, in violation of the users' privacy rights.

157. By embedding the tracking technologies on its Website and disclosing the content of federal employee communications relating to symptoms, conditions, treatments, doctors, and other Sensitive Information, Defendant had a purpose that was tortious, criminal, and designed to violate state and federal laws including:

a. An invasion of privacy through public disclosure of private facts;

b. A violation of 42 U.S.C. § 1320d-6, the Administrative Simplification subtitle of HIPAA, which protects against the disclosure of individually identifiable health information to another person and is a criminal offense punishable by fine or imprisonment;

c. A violation of HIPAA; and

d. A violation of Illinois's computer tampering statute. 720 ILCS 5/17-51(a)(1)-(2), (a)(4).

158. 42 U.S.C. § 1320d-6 provides criminal and civil penalties against a healthcare provider who "knowingly . . . discloses individually identifiable health information to another

person." Section 1320d(6) of HIPAA defines individually identifiable health information ("IIHI") as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and—(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

42 U.S.C. § 1320d(6).

159. Guidance issued by the Department of Health and Human Services confirms that the type of online tracking technologies deployed by Defendant violates HIPAA. HIPAA prohibits disclosing patients' health information via tracking technologies on both user-authenticated webpages (such as the log-in portal) and unauthenticated webpages. The guidance includes IP addresses, device IDs, and unique identifying codes collected on a regulated entity's website in the definition of IIHI. As described above, Plaintiffs entered data on Defendants' website relating to their private medical issues and some later received advertisements from BCBS. This shows that through the tracking technologies employed, Defendant disclosed federal employees' individually identifiable health information to third parties in violation of the ECPA.

160. Defendant was not acting under color of law to intercept Plaintiffs' and the Class Members' wire or electronic communications.

161. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' privacy via the tracking technologies. Nor did Plaintiffs and Class Members consent to the disclosure of their sensitive medical information to unauthorized third parties.

162. A person who violates § 2511(1)(a) is liable for $10,000 in statutory damages to any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used.

163. Defendant is liable to Plaintiffs and Class Members for violations of the ECPA.

164. Based on the foregoing, Plaintiffs and Class Members seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

COUNT II
VIOLATION OF THE ILLINOIS EAVESDROPPING STATUTE ("IES") 720 ILCS § 5/14-1, et seq.
(On Behalf of Plaintiffs and the Nationwide Class)

165. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

166. The Illinois Eavesdropping Statute ("IES"), 720 ILCS § 5/14-1, *et seq.*, prohibits the surreptitious interception, recording, or transcription of private electronic communications without the consent of all parties to the conversation and provides a civil cause of action to a person subjected to a violation of the IES against eavesdroppers and their principals.

167. The IES makes it unlawful for a person to knowingly and intentionally intercept, record, or transcribe, in a surreptitious manner, any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication. 720 ILCS § 5/14-2(a)(3).

168. The IES makes it unlawful for a person to knowingly and intentionally use or disclose any information which he or she knows or reasonably should know was obtained from a

private conversation or private electronic communication in violation of the IES, unless he or she does so with the consent of all of the parties. 720 ILCS § 5/14-2(a)(5).

169. The IES makes it unlawful for a person to knowingly and intentionally "possesses any electronic, mechanical, eavesdropping, or other device knowing that or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious overhearing, transmitting, or recording of private conversations or the interception, or transcription of private electronic communications and the intended or actual use of the device is contrary to the provisions of" the IES. 720 ILCS § 5/14-2(a)(4).

170. The IES creates a private cause of action for "[a]ny or all parties to any conversation or electronic communication upon which eavesdropping is practiced contrary to" the IES. 720 ILCS § 5/14-6.

171. IES defines "private 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, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation." 720 ILCS § 5/14-1(e).

172. "Surreptitious," as used in the IES, "means obtained or made by stealth or deception, or executed through secrecy or concealment." 720 ILCS § 5/14-1(g).

173. An "eavesdropper" means "any person . . . who operates or participates in the operation of any eavesdropping device contrary to the provisions of [the IES] or who acts as a principal[.]" 720 ILCS § 5/14-1(b).

174. A "principal" includes any person who "[k]owingly derives any benefit or information from the illegal use of an eavesdropping device by another" or "[d]irects another to use an eavesdropping device illegally on his or her behalf." 720 ILCS § 5/14-1(c).

175. An "eavesdropping device" is "any device capable of being used to . . . intercept . . . electronic communications[.]" 720 ILCS § 5/14-1(a).

176. Plaintiffs' and the Class's communications with Defendant constituted private electronic communications. Plaintiffs and the Class transmitted their communications to Defendant by wire and from their computers or other electronic devices, intended the communications to be private, and reasonably expected the communications to be private given the sensitivity of the information communicated and HIPAA's prohibition on unauthorized disclosure of IIHI to third parties.

177. TikTok, Meta, Google, and LinkedIn were not parties to Plaintiffs' and the Class's private electronic communications with Defendant. Plaintiffs and the Class believed they were only communicating with Defendant, intended for their communications to be directed at Defendant only, and were unaware of the presence of concealed tracking technology code that redirected their communications to third parties.

178. TikTok, Meta, Google, and LinkedIn's interceptions of Plaintiffs' and Class Members' private electronic communications were knowing, intentional, and surreptitious. TikTok, Meta, Google, and LinkedIn intentionally designed their tracking code so that it could be deployed on websites to secretly intercept private communications. TikTok, Meta, Google, and LinkedIn knew that their tracking code was capable of, and in fact did, intercept private electronic communications without the consent of all parties to the communication.

179. On information and belief, TikTok, Meta, Google, and LinkedIn used and disclosed Plaintiffs' and the Class' intercepted communications for advertising purposes, consistent with their advertising and data-monetization business models.

180. Plaintiffs and the Class did not consent to the interception, recording, or transcription by third parties of their private electronic communications with Defendant.

181. Defendant knowingly and intentionally acted as TikTok, Meta, Google, and LinkedIn's "principal" under the IES. By deploying the tracking technology code from TikTok, Meta, Google, and LinkedIn on its Website, Defendant directed that TikTok, Meta, Google, and LinkedIn illegally eavesdrop on Plaintiffs' private electronic communications on its behalf. Defendant also knowingly and intentionally derived benefits and information from the illegal eavesdropping, including data about visitor activities on its Website Defendant could use to improve its advertising and marketing campaigns and improve its data analytics.

182. Defendant also knowingly and intentionally used information it knew or reasonably should have known was obtained from a private electronic communication without the consent of Plaintiffs and the Class in violation of 720 ILCS § 5/14-2(a)(5), by using the intercepted information for its own marketing, advertising, and data analytics purposes.

183. Defendant further violated 720 ILCS § 5/14-2(a)(4) by possessing the tracking code, knowing that its design rendered it primarily useful for surreptitiously intercepting private electronic communications contrary to the IES.

184. Defendant's violations of the IES were committed with wanton disregard of Plaintiffs' and Class Members' rights.

185. For Defendant's violations of the IES, Plaintiffs and Class members seek actual damages, punitive damages, injunctive relief, and any other relief the Court deems just.

COUNT III
VIOLATION OF THE ILLINOIS COMPUTER TAMPERING ACT ("ICTA") 720 ILCS § 5/17-51
(On Behalf of Plaintiffs and the Nationwide Class)

186. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

187. The Illinois Computer Tampering Act ("ICTA") prohibits any person from knowingly and without the authorization of a computer's owner or in excess of the authority granted him or her from inserting or attempting to insert a program into a computer or computer program knowing or having reason to know that such program contains information or commands that will or may alter or remove data from that computer or cause loss to the users of that computer. 720 ILCS § 5/17-51(a)(4).

188. The ICTA provides that, "[w]hoever suffers loss by reason of a violation of subdivision (a)(4) of [the ICTA] may, in a civil action against the violator, obtain appropriate relief. In a civil action under [the ICTA], the court may award to the prevailing party reasonable attorney's fees and other litigation expenses." 720 ILCS § 5/17-51(c).

189. Defendant knowingly and without authorization of Plaintiffs and the Class inserted and attempted to insert tracking code from TikTok, Meta, Google, and LinkedIn into the computers and browsers of Plaintiffs and the Class.

190. Defendant inserted and attempted to insert the tracking code knowing or having to reason to know that the tracking code contained information or commands that would or could alter or remove data from Plaintiffs' and the Class's computers and browsers, including by directing Plaintiffs' and the Class's computers and browsers to simultaneously redirect communications intended only for Defendant to TikTok, Meta, Google, and LinkedIn.

191. Defendant also knew or should have known that the tracking code would or could cause loss to Plaintiffs and the Class by resulting in disclosure of their Sensitive Information to unauthorized third parties from whom Plaintiffs and the Class could not retrieve the data or otherwise regain control of their personal information.

192. Because the tracking code operated surreptitiously and without Plaintiffs' and the Class's knowledge, awareness, and consent, Defendant's deployment of the tracking code was done without the authorization of Plaintiffs and the Class.

193. Defendant's violations of the ICTA were committed with wanton disregard of Plaintiffs' and Class Members' rights.

194. For Defendant's violations of the ICTA, Plaintiffs and Class members seek actual damages, punitive damages, injunctive relief, attorneys' fees, litigation expenses, and any other relief the Court deems just.

COUNT IV
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA") Cal. Penal Code § 630, *et seq.*
(On behalf of Plaintiff Gouch and the California Class)

195. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

196. The California Invasion of Privacy Act ("CIPA") is codified at California Penal Code §§ 630 to 638.

197. CIPA begins with its statement of purpose:

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

Cal. Pen. Code § 630.

198. California Penal Code § 631(a) imposes liability on:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section . . . .

199. At all relevant times, Defendant has been a "person" within the scope of CIPA. Cal. Penal Code §631(a).

200. Defendant aided, employed, agreed with, and conspired with TikTok and other third-party technology companies to track and intercept Plaintiffs' and the Class Members' internet communications while using Defendant's Website. Defendant's conduct allowed unauthorized third parties to read and learn about the contents or meaning of any message, report, or communication from Plaintiffs and the California Class while the same was in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within California.

201. Defendant intentionally inserted an electronic device (the tracking technology code) that, without the knowledge and consent of Plaintiffs and the California Class, recorded and transmitted their confidential communications with Defendant to third parties.

202. Defendant willfully facilitated and aided the interception and collection of Plaintiffs' and the California Class's Sensitive Information by embedding the tracking code on the Website.

203. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the tracking code falls under the broad catch-all category of "any other manner":

a. The computer codes and programs TikTok, Meta, Google, and LinkedIn used to track Plaintiffs' and the California Class's communications while they were navigating the Website;

b. Plaintiffs' and the California Class's browsers;

c. Defendant's Website and webserver;

d. Plaintiffs' and the California Class's computing and mobile devices;

e. The web and ad servers from which TikTok, Meta, Google, and LinkedIn tracked and intercepted Plaintiffs' and the California Class's communications while they were using a web browser to access or navigate the Website;

f. The computer codes and programs used by TikTok, Meta, Google, and LinkedIn to effectuate its tracking and interception of Plaintiffs' and the California Class's communications while they were using a browser to visit the Website; and

g. The plan Defendant, TikTok, Meta, Google, and LinkedIn carried out to effectuate their tracking and interception of Plaintiffs' and the California Class's communications while they were using a web browser to visit the Website.

204. As a result of the above violations and pursuant to CIPA Section 637.2, Defendant is liable to Plaintiffs and the California Class for the greater of: a) treble actual damages related to their loss of privacy in an amount to be determined at trial; or b) for statutory damages in the amount of $5,000 per violation. Section 637.2 specifically states that "[i]t is not a necessary

prerequisite to an action pursuant to this section that the Plaintiff has suffered, or be threatened with, actual damages."

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

206. Based on the foregoing, Plaintiffs and the California Class seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

COUNT V
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

207. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

208. At all relevant times, Defendant owed Plaintiffs and Class Members a duty to act with reasonable care to secure and safeguard their Sensitive Information from unauthorized disclosure to third parties. Defendant took on this obligation by soliciting and obtaining Sensitive Information from Plaintiffs and the Class on its Website and maintaining the information on its system and networks.

209. Among these duties, Defendant was expected:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Sensitive Information in its possession;

b. To protect Plaintiffs' and Class Members' Sensitive Information using reasonable and adequate security procedures and systems compliant with industry-standard practices;

c. To implement processes to quickly detect unauthorized disclosures and to timely act on warnings about such disclosures; and

d. To promptly notify Plaintiffs and Class Members of any unauthorized disclosure that affected or may have affected their Sensitive Information.

210. It was reasonably foreseeable and highly likely that disclosure of federal employees' Sensitive Information to third-party technology companies would cause a loss of privacy and loss of control over employees' personal medical data. It was especially foreseeable and likely that disclosing federal employees' sensitive medical information to TikTok would violate employees' privacy interests and raise national security concerns given the U.S. government's efforts to ban the use of TikTok on official government devices and systems.

211. Defendant's services did not depend on Defendant deploying the tracking code from TikTok, Meta, Google, and LinkedIn on its Website. The magnitude of the burden on Defendant to prevent the disclosure of federal employees' Sensitive Information to third-party technology companies is and was minimal, as reflected in federal guidance and HIPAA provisions prohibiting such disclosure.

212. The consequences of placing the burden on Defendant to prevent disclosure of federal employees' Sensitive Information to third-party technology companies are and were likewise minimal. At all relevant times, Defendant had ultimate control over the source code it deployed on its Website, and Defendant was able to provide healthcare services to federal employees without the use of the tracking code from TikTok, Meta, Google, and LinkedIn.

213. Defendant breached its duty of care to Plaintiffs and the Class in the following ways, among others:

a. By failing to implement adequate data-security protocols to prevent the unauthorized disclosure of Sensitive Information collected via the Website;

b. By failing to adhere to industry standards regarding the safeguarding of Sensitive Information and the use of online tracking technologies;

c. By installing and deploying the tracking source code and failing to monitor and prevent the collection and dissemination of Sensitive Information intercepted through the tracking source code;

d. By failing to adequately train IT staff, network security personnel, and/or marketing and advertising personnel to safeguard and protect from disclosure employees' Sensitive Information; and

e. By failing to implement processes to detect and respond to unauthorized disclosures involving Sensitive Information and promptly notify affected employees.

214. As a direct and proximate result of Defendant's breach and unauthorized disclosure of Plaintiffs' and the Class's Sensitive Information, Plaintiffs and Class Members suffered and continue to suffer harm and injury, including loss of privacy associated with disclosure of their sensitive medical data and the loss of the benefit of the bargain. Had Plaintiffs and the Class known that Defendant secretly disclosed their Sensitive Information to third parties—including TikTok—they would have used the services of another insurance provider under the FEHB program or paid or demanded a lower price for Defendant's services.

215. Plaintiffs and the Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages in an amount to be proven at trial.

COUNT VI
INVASION OF PRIVACY – PUBLICATION OF PRIVATE FACTS
(On Behalf of Plaintiffs and the Nationwide Class)

216. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

217. A claim for invasion of privacy by publication of private facts requires that (1) publicity was given to the disclosure of private facts; (2) the facts were private and not public facts; and (3) the matter made public would be highly offensive to a reasonable person.

218. Defendant's conduct in deploying the tracking code from TikTok, Meta, Google, and LinkedIn on its Website resulted in the publication of private facts to the largest digital advertising companies in the world. On information and belief, TikTok, Meta, Google, and LinkedIn aggregated Plaintiffs' and the Class's personal and highly sensitive medical data for purposes of selling targeted advertising and/or otherwise monetizing the data in the broader data marketplace, consistent with their business models, resulting in the widespread publication of Plaintiffs' and the Class's data.

219. Plaintiffs' and the Class's communications of Sensitive Information regarding symptoms, conditions, and treatments were private and intended only for Defendant.

220. Defendant's publication of Plaintiffs' and the Class's Sensitive Information obtained via the Website is highly offensive to a reasonable person because the tracking was entirely surreptitious, and the disclosures relate to federal employees' most sensitive personal information, including information about specific symptoms, conditions, and treatments. The disclosure is also highly offensive because it violates HIPAA and regulatory guidance. The publication to TikTok is particularly highly offensive given the U.S. Government's efforts to prevent disclosure of sensitive information to TikTok.

221. As a direct and proximate result of Defendant's unauthorized disclosure of Plaintiffs' and the Class's private medical data, Plaintiffs and Class Members suffered and continue to suffer harm and injury, including loss of privacy associated with disclosure of their sensitive medical data and the loss of the benefit of the bargain. Had they known that Defendant secretly disclosed their Sensitive Information to third parties—including TikTok—they would have used the services of another insurance provider under the FEHB program or paid or demanded a lower price for Defendant's services.

222. Plaintiffs and the Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages in an amount to be proven at trial.

COUNT VII
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

223. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

224. When Plaintiffs and Class Members paid money and provided their Sensitive Information to Defendant in exchange for services, they entered implied contracts pursuant to which Defendant agreed to safeguard and not disclose their Sensitive Information without Plaintiffs' and Class Members' consent.

225. An implicit part of the agreement was that Defendant would safeguard Plaintiffs' and Class Members' Sensitive Information consistent with industry and regulatory standards and state and federal law and would timely notify Plaintiffs in the event of a disclosure to third parties.

226. Plaintiffs and Class Members would not have entrusted Defendant with their Sensitive Information in the absence of an implied contract between them and Defendant obligating Defendant not to disclose this information without consent.

227. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

228. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Sensitive Information to various third parties, including TikTok, Meta, Google, and LinkedIn.

229. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members would not have used Defendant's services, or would have paid substantially less for these services, had they known their sensitive health-related information would be disclosed.

230. Plaintiffs and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breaches of implied contract.

COUNT VIII
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class)

231. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

232. Plaintiffs and Class Members provided their Sensitive Information to Defendant for the purposes of receiving healthcare services or healthcare-related information and knowledge. Defendant receives a benefit from its use of Plaintiffs' and the Class Members' Sensitive Information, including costs savings for marketing and advertising and increased profits from the acquisition of new patients and existing patients seeking more services. Defendant intentionally collected and used Plaintiffs' and the Class Members' Sensitive Information for its own gain, without consent or authorization.

233. Defendant unjustly retained those benefits at the expense of Plaintiffs and the Class Members and this conduct damaged Plaintiffs and the Class Members. Plaintiffs and the Class Members were not compensated by Defendant for the data they provided.

234. It would be inequitable and unjust for Defendant to retain any of the profit or other benefits derived from the secret, unfair, and deceptive data tracking methods Defendant employs on its Website.

235. The Court should require Defendant to disgorge all unlawful or inequitable proceeds that it received into a common fund for the benefit of Plaintiffs and Class Members, and order other such relief as the Court may deem just and proper.

236. Plaintiffs allege this claim in the alternative in the event Plaintiffs and Class Members have an inadequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully pray for judgment in their favor as follows:

a. Certification of the Classes pursuant to the provisions of Fed. R. Civ. P. 23 and an order that notice be provided to all Class Members;

b. Designation of Plaintiffs as representatives of the Classes and the undersigned counsel as Class Counsel;

c. An award of damages in an amount to be determined at trial or by this Court;

d. An order for injunctive relief, enjoining Defendant from engaging in the wrongful and unlawful acts described herein;

e. An order for declaratory relief as may be appropriate;

f. An award of statutory interest and penalties;

g. An award of costs and attorneys' fees; and

h. Such other relief the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiffs hereby demand a trial by jury of all issues so triable.

Respectfully submitted,

Dated: November 7, 2023

/s/ David M. Cialkowski

David M. Cialkowski, IL Bar No. 6255747
Brian C. Gudmundson
Jason P. Johnston
Rachel K. Tack
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
david.cialkowski@zimmreed.com
brian.gudmundson@zimmreed.com
jason.johnston@zimmreed.com
rachel.tack@zimmreed.com

Hart L. Robinovitch
Ryan J. Ellersick
ZIMMERMAN REED LLP
14648 N. Scottsdale Road, Suite 130
Scottsdale, AZ 85254
Telephone: (480) 348-6400
Facsimile: (480) 348-6415
hart.robinovitch@zimmreed.com
ryan.ellersick@zimmreed.com

Attorneys for Plaintiffs

ClassAction.org
