Michael J. Manning, Esq. (SBN 286879)
MANNING LAW, APC
26100 Towne Centre Drive
Foothill Ranch, CA 92610
Office: (949) 200-8755
Email: privacy@manninglawoffice.com

Reuben D. Nathan, Esq. (SBN 208436)
NATHAN & ASSOCIATES, APC
2901 W. Coast Hwy., Suite 200
Newport Beach, CA 92663
Office: (949) 270-2798
Email: rnathan@nathanlawpractice.com

Ross Cornell, Esq. (SBN 210413)
LAW OFFICES OF ROSS CORNELL, APC
40729 Village Dr., Suite 8 - 1989
Big Bear Lake, CA 92315
Office: (562) 612-1708
Email: rc@rosscornelllaw.com

Attorneys for Plaintiff: JOHN TASKER

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JOHN TASKER, an individual,

Plaintiff,

v.

TRUIST FINANCIAL CORPORATION, a North Carolina corporation, and DOES 1-10, inclusive,

Defendants.

Case No:

COMPLAINT
1. Cal. Penal Code § 638.51
2. Cal. Constitution Art. I § 1
3. Cal. Civil Code § 1798.100, *et seq.*
4. Cal. Bus. & Prof. Code § 17200, *et seq.*
5. Intrusion Upon Seclusion
6. Unjust Enrichment

CLASS ACTION

I. NATURE OF THE ACTION

1. Defendant TRUIST FINANCIAL CORPORATION ("Defendant" or "TRUIST") owns and operates a website, www.truist.com (the "Website").

2. This is a class action lawsuit brought by Plaintiff on behalf of himself and on behalf of all California residents who have accessed the Website.

3. Plaintiff JOHN TASKER files this class action complaint on behalf of himself and all others similarly situated (the "Class Members") against Defendant. Plaintiff brings this action based upon personal knowledge of the facts pertaining to him, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

4. A pixel tracker, also known as a web beacon, is a tracking mechanism embedded in a website that monitors user interactions. It typically appears as a small, transparent 1x1 image or a lightweight JavaScript snippet that activates when a webpage is loaded or a user performs a tracked action.

5. When triggered, the pixel transmits data from the user's browser to a third-party server. This data typically includes page views, session duration, referrer URLs, IP address, browser and device details, and other interaction metadata.

6. When users visit the Website, Defendant causes tracking technologies to be embedded in visitors' browsers. These include, but are not limited to, the following:

- Adobe DTM
- Qualtrics Tracker
- Facebook Tracker
- Google Ads / DoubleClick
- AdRoll Tracker
- The Trade Desk Tracker
- Microsoft Ads

7. The third parties who operate the above-listed trackers use pieces of User Information (defined below) collected via the Website as described herein for their own

independent purposes tied to broader advertising ecosystems, profiling, and data monetization strategies that go beyond Defendant's direct needs for their own financial gain. The above-listed trackers, together with the additional trackers identified on **Exhibit A** to this Complaint (which are incorporated by reference herein), are referred to herein collectively as the "Trackers."

8. The Trackers are operated by distinct third parties: Adobe, Inc. (Adobe DTM); Qualtrics International, Inc. (Qualtrics Tracker); Meta Platforms, Inc. (Facebook Tracker); Google LLC (Google Ads/DoubleClick); NextRoll, Inc. (AdRoll); The Trade Desk, Inc. (The Trade Desk Tracker); and Microsoft Corporation (Microsoft Ads). Defendant enables these trackers, which transmit user data to third-party servers to identify users and support advertising, profiling, and data monetization activities.

9. Through the Trackers, the Third Parties collect detailed user information including IP addresses, browser and device type, screen resolution, operating system, pages visited, session duration, scroll depth, mouse movements, click behavior, referring URLs, unique identifiers (such as cookies and ad IDs), and geolocation based on IP. This information is used for behavioral profiling, ad targeting, cross-device tracking, and participation in real-time advertising auctions.

10. Because the Trackers capture and transmit users' IP addresses, full page URLs, referrer headers, device identifiers, and other non-content metadata, they function as "pen registers" and/or "trap and trace devices" under Cal. Penal Code § 638.50. These tools silently collect routing and addressing information for commercial use without user interaction, as defined in *Greenley v. Kochava, Inc.*, 2023 WL 4833466 (S.D. Cal. July 27, 2023).

11. Plaintiff and the Class Members did not consent to the installation, execution, embedding, or injection of the Trackers on their devices and did not expect their behavioral data to be disclosed or monetized in this way. By installing and using the Trackers without prior consent and without a court order, Defendant violated CIPA section 638.51.

12. By installing and activating the Trackers without obtaining user consent or a valid court order, Defendant violated California Penal Code § 638.51, which prohibits the use of pen registers and trap and trace devices under these circumstances.

13. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of California residents.

14. Generalized references herein to users, visitors and consumers expressly include Plaintiff and the Class Members.

II. PARTIES

15. Plaintiff JOHN TASKER ("Plaintiff") is a California citizen residing in San Bernardino County and has an intent to remain there. Plaintiff was in California when he visited the Website, which occurred on multiple instances during the class period prior to the filing of the complaint in this matter. The allegations set forth herein are based on the Website as configured when Plaintiff visited it.

16. Defendant TRUIST FINANCIAL CORPORATION is a North Carolina corporation that owns, operates and/or controls the Website which is an online platform that offers goods and services to consumers.

17. TRUIST is one of the largest financial services companies in the United States, formed through the 2019 merger of BB&T Corporation and SunTrust Banks, Inc. Headquartered in Charlotte, North Carolina, TRUIST provides a wide range of services including retail and commercial banking, insurance, wealth management, and capital markets solutions. As of recent filings, it holds hundreds of billions in assets and operates across a broad geographic footprint, primarily in the southeastern and mid-Atlantic regions of the U.S.

18. Truist Bank is the flagship banking subsidiary of TRUIST. It holds the federal banking charter and is the legal entity responsible for most deposit-taking, lending, and regulatory compliance activities. Truist Bank is directly overseen by financial regulatory bodies including the FDIC and Federal Reserve and carries out the operational banking functions on behalf of the broader holding company.

19. The Website serves as the primary digital gateway for the company's banking and financial services. It functions as a centralized platform for customers to access personal and business banking tools, apply for loans, find branches, manage accounts, and interact with various products and services offered by TRUIST. In addition to its operational role, the website also plays a major role in customer engagement, advertising, and data collection — which makes its tracking and privacy practices significant from a compliance standpoint, particularly under CIPA and related privacy laws.

III. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because the total matter in controversy exceeds $5,000,000 and there are over 100 members of the proposed class. Further, at least one member of the proposed class is a citizen of a State within the United States and at least one defendant is the citizen or subject of a foreign state.

21. This Court has personal jurisdiction over Defendant because, on information and belief, Defendant has purposefully directed its activities to the Central District of California by regularly engaging with individuals in California through its website. Defendant's illegal conduct is directed at and harms California residents, including Plaintiff, and if not for Defendant's contact with the forum, Plaintiff would not have suffered harm.

22. Venue is proper in the Central District of California pursuant to 28 U.S.C. § 1391 because Defendant (1) is authorized to conduct business in this District and has intentionally availed itself of the laws and markets within this District; (2) does substantial business within this District; (3) is subject to personal jurisdiction in this District because it has availed itself of the laws and markets within this District; and (4) the injury to Plaintiff occurred within this District.

/ /

/ /

IV. GENERAL ALLEGATIONS

1. *The California Invasion of Privacy Act (CIPA)*

23. Enacted in 1967, the California Invasion of Privacy Act (CIPA) is a legislative measure designed to safeguard the privacy rights of California residents by prohibiting unauthorized wiretapping and eavesdropping on private communications. The California Legislature recognized the significant threat posed by emerging surveillance technologies, stating that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society" (Cal. Penal Code § 630).

24. CIPA specifically prohibits the installation or use of "pen registers" and "trap and trace devices" without consent or a court order (Cal. Penal Code § 638.51(a)).

25. A "pen register" is defined as a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, excluding the contents of the communication (Cal. Penal Code § 638.50(b)).

26. Conversely, a "trap and trace device" captures incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, again excluding the contents (Cal. Penal Code § 638.50(b)).

27. In practical terms, a pen register records outgoing dialing information, while a trap and trace device records incoming dialing information.

28. Historically, law enforcement has utilized these devices to monitor telephone calls, with pen registers recording outgoing numbers dialed from a specific line and trap and trace devices recording incoming call numbers to that line.

29. Although originally focused on landline telephone calls, CIPA's scope has expanded to encompass various forms of communication, including cell phones and online interactions. For instance, if a user sends an email, a pen register could record

the sender's email address, the recipient's email address, and the subject line—essentially capturing the user's outgoing information.

30. Similarly, if the user receives an email, a trap and trace device could record the sender's email address, the recipient's email address, and the subject line—capturing the incoming information.

31. Despite predating the Internet, CIPA has been interpreted by the California Supreme Court to apply to new technologies where such application does not conflict with the statutory scheme (*In re Google Inc.*, 2013 WL 5423918, at *21; *Greenley*, supra, 2023 WL 4833466, at *15; *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1). This interpretation aligns with the principle that CIPA should be construed to provide the greatest privacy protection when faced with multiple possible interpretations (*Matera v. Google Inc.*, 2016 WL 8200619, at *19).

32. The conduct alleged herein constitutes a violation of a legally protected privacy interest that is both concrete and particularized. Invasions of privacy have long been actionable under common law. (*Patel v. Facebook*, 932 F.3d 1264, 1272 (9th Cir. 2019); Eichenberger v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017).)

33. Both the legislative history and statutory language indicate that the California Legislature intended CIPA to protect core privacy rights. Courts have found that violations of CIPA give rise to concrete injuries sufficient to confer standing under Article III. (See *Campbell v. Facebook, Inc.*, 2020 WL 1023350; *In re Facebook Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020).)

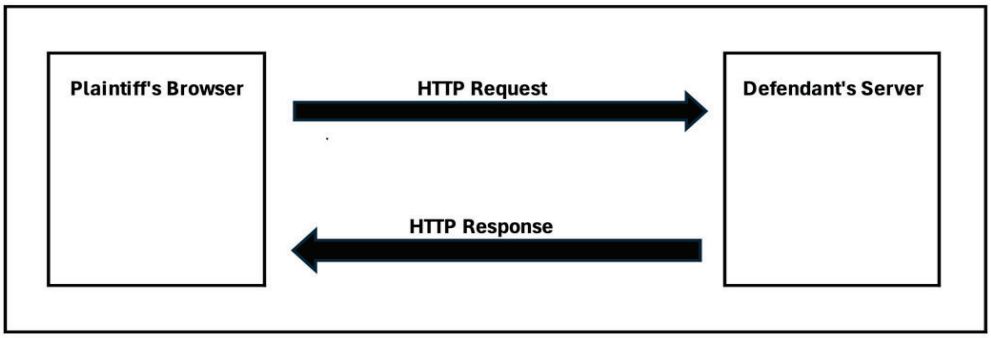
34. Individuals may pursue legal action against violators of any CIPA provision, including Section 638.51, and are entitled to seek $5,000 in statutory penalties per violation (Cal. Penal Code § 637.2(a)(1)).

2. *The Trackers Are "Pen Registers" and/or "Trap and Trace Devices"*

35. When the Plaintiff and Class Members accessed the Website, their browsers initiated an HTTP or HTTPS request to Defendant's web server, which hosts the content and functionality of the site. In response, the server transmitted an HTTP

response containing the necessary resources—including HTML, cascading style sheets (CSS), JavaScript files, and image assets—used by the browser to render and display the webpage. These resources also included client-side scripts that initiate communication with third-party services for analytics, marketing, and tracking purposes. ***Figure 1*** below illustrates sample HTTP requests.

Figure 1



36. The server's response included third-party tracking scripts that were executed by the Plaintiff's and Class Members' web browsers. These scripts, once executed, initiate client-side functions that capture routing and behavioral metadata and transmit this data — typically via HTTPS requests — to the servers of third-party tracking vendors. These actions occur without visible indicators or user awareness. The transmitted data—referred to as User Information—included identifiers such as IP addresses, device characteristics, browser types, page navigation behavior, and unique tracking cookies, all of which were used to profile users and facilitate targeted advertising.

37. The Trackers operate by initiating HTTP or HTTPS requests—using either the GET or POST method—from the user's browser to external servers controlled by the Third Parties. These requests are triggered by user interactions with the Website and are used to transmit behavioral data and device metadata, including information such as page views, click events, session duration, and identifying browser characteristics.

38. An Internet Protocol (IP) address is a numerical identifier assigned to each device or network connected to the Internet, used to facilitate communication between systems. *See hiQ Labs, Inc. v. LinkedIn Corp.* (9th Cir. 2019) 938 F.3d 985, 991 n.4. The most common format, known as IPv4, consists of four numbers separated by periods (e.g., 191.145.132.123). IP addresses enable routing of data between devices and can be used—via external geolocation services—to infer a user's general location, including state, city, and in some cases, ZIP code.

39. Public IP addresses are unique identifiers assigned by Internet Service Providers (ISPs) that allow devices to communicate directly over the Internet. They are globally accessible, meaning they can be reached from anywhere on the Internet, but are not inherently exposed unless data is being transmitted. Public IP addresses are essential for devices requiring direct Internet access and can be used to approximate a device's physical location through geolocation services.

40. In contrast, private IP addresses are used within internal networks and are not routable on the public Internet. They are isolated from the global Internet and can be reused across different networks without conflict. Unlike public IP addresses, private IP addresses do not divulge a user's geolocation.

41. Public IP addresses play a significant role in digital marketing by enabling geographic targeting based on a user's approximate location. Through IP geolocation services, advertisers can often determine a user's country, region, city, and in some cases, ZIP code or service area. In contexts where a static IP address is associated with a fixed residence or business, this data can contribute to household-level or business-level targeting—particularly when combined with other tracking identifiers and third-party enrichment.

42. A public IP address functions as "routing, addressing, or signaling information" by facilitating internet communication. It provides essential information that can help determine the general geographic coordinates of a user accessing a website through geolocation databases. Additionally, a public IP address is involved in routing

communications from the user's router to the intended destination, ensuring that emails, websites, streaming content, and other data reach the user correctly.

43. As "routing, addressing, or signaling information," a public IP address is indispensable for maintaining seamless and efficient communication over the Internet. It ensures that data packets are sent from the user's router to the intended destination, such as a website or email server.

44. Defendant installs Trackers on users' browsers to collect User Information, including IP addresses and full URLs, which constitute outgoing routing and addressing metadata under CIPA. These identifiers serve the same function as telephony dialed numbers and therefore meet the statutory definition of a pen register or trap and trace device.

3. *The Use of Pixel Trackers or Beacons and Digital Fingerprinting*

45. Website users typically expect a degree of anonymity when browsing, particularly when they are not logged into an account. However, upon visiting the Website, Plaintiff's and Class Members' browsers executed third-party tracking scripts embedded by the Defendant. These Trackers operate in the background of the browsing session and collect detailed behavioral and technical information, which is then transmitted to external third-party servers without the users' active awareness.

46. This process, known as digital fingerprinting, involves compiling various data points—such as browser version, screen resolution, installed fonts, device type, and language settings—to generate a unique identifier for each user. Fingerprinting can be used to recognize repeat visits and correlate activity across different sessions or sites. When combined with form inputs, login activity, or third-party enrichment, fingerprinting can contribute to broader profiling of a user's interests, affiliations, or behaviors.

47. When combined with additional tracking mechanisms—such as cookies, login data, and third-party enrichment services—fingerprinting contributes to user profiling. This may include inferring location, browsing habits, consumer preferences,

and potentially associating these patterns with known user identities. A sufficiently detailed digital fingerprint—especially when correlated with other identifiers such as email addresses, form submissions, or third-party databases—can enable the reidentification of a user.

48. The ability to associate a persistent digital profile with a specific individual—using techniques such as digital fingerprinting—has led to the development of a data industry known as identity resolution. Identity resolution involves recognizing users across sessions, devices, and platforms by connecting various identifiers derived from their digital behavior, including IP addresses, browser metadata, cookies, and, in some cases, login credentials. The process may occur deterministically (based on known logins or user-submitted information) or probabilistically (based on behavioral or technical similarity).

49. In simpler terms, pen register and trap and trace mechanisms in the digital context refer to technologies that record metadata such as IP addresses, URLs visited, and device characteristics—information that identifies the routing and addressing of electronic communications. This can be achieved through the deployment of tracking technologies like the Trackers installed, executed, embedded or injected in the Website, which operate without user interaction or visibility.

50. The Trackers provide analytics and marketing services to Defendant using the data collected from visitors to the Website when they visited the Website and from when they visited other websites that included the pen register and trap and trace devices.

51. When users visit the Website, installed, executed, embedded or injected Trackers initiate network requests to third-party servers, using invisible image pixels, JavaScript calls, or beacon APIs. These requests include the user's IP address, which is transmitted automatically as part of the HTTP request header. In many cases, the Tracker's server responds by placing a persistent cookie in the user's browser, which serves as a unique identifier that can be used to recognize and track the user across

future visits. If a user deletes their browser cookies, this identifier is removed. However, upon revisiting the Website, the process repeats: the browser executes the Tracker's script, a new identifier is set, and the Tracker resumes collecting the user's IP address and associated behavioral data.

4. *Plaintiff's And Class Members' Data Has Financial Value*

52. Given the number of Internet users, the "world's most valuable resource is no longer oil, but data."[1]

53. Consumers' web browsing histories have an economic value more than $52 per year, while their contact information is worth at least $4.20 per year, and their demographic information is worth at least $3.00 per year.[2]

54. There is a "a study that values users' browsing histories at $52 per year, as well as research panels that pay participants for access to their browsing histories."[3]

55. Extracted personal data can be used to design products, platforms, and marketing techniques. A study by the McKinsey global consultancy concluded that businesses that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[4]

56. In 2013, the Organization for Economic Cooperation and Development ("OECD") estimated that data trafficking markets had begun pricing personal data, including those obtained in illicit ways without personal consent. It found that illegal markets in personal data valued each credit cardholder record at between 1 and 30 U.S.

---

[1] Ian Cohen, Are Web-Tracking Tools Putting Your Company at Risk?, Forbes (Oct 19, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/10/19/are-web-tracking-tools-putting-your-company-atrisk/?sh=26481de07444

[2] *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 928 (N.D. Cal. 2015), rev'd, 956 F.3rd 589 (9th Cir. 2020).

[3] *In re Facebook, Inc. Internet Tracking Litigation* (9th Cir. 2020) 956 F.3rd 589, 600.

[4] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, Capturing value from your customer data, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/businessfunctions/quantumblack/ourinsights/capturing-value-from-your-customer-data

dollars in 2009, while bank account records were valued at up to 850 U.S. dollars. Data brokers sell customer profiles of the sort that an online retailer might collect and maintain for about 55 U.S. dollars, and that individual points of personal data ranged in price from $0.50 cents for an address, $2 for a birthday, $8 for a social security number, $3 for a driver's license number, and $35 for a military record (which includes a birth date, an identification number, a career assignment, height, weight, and other information). Experiments asking individuals in the United States and elsewhere how much they value their personal data points result in estimates of up to $6 for purchasing activity, and $150-240 per credit card number or social security number.[5]

57. The last estimate probably reflects public reporting that identify theft affecting a credit card number or social security number can result in financial losses of up to $10,200 per victim.[6]

58. The Defendant's monetization of personal data constitutes actionable economic harm under federal law, even without evidence of a direct financial loss, as a "misappropriation-like injury" caused by converting user data into a revenue stream through targeted advertising. *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020).

5. *Defendant Is Motivated To Monetize Consumer Information Regardless of Consent*

59. By implementing Trackers on the Website, Defendant participates in building detailed behavioral profiles of visitors. These profiles include information such as which users viewed specific products, whether they initiated but abandoned the checkout process, and what pages or buttons they interacted with. This data enables

[5] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220 (Apr. 2, 2013), at 27-28, https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf

[6] Bradley J. Fikes, Identity Theft Hits Millions, Report Says, San Diego Union Tribune, Sept. 4, 2003, https://www.sandiegouniontribune.com/sdut-identity-theft-hits-millions-report-says-2003sep04-story.html.

Defendant and its advertising partners to identify repeat visits from the same device or browser. This behavioral data is integrated into third-party advertising platforms, allowing Defendant to deliver retargeted ads to users who previously visited the Website, offer promotional incentives to users who showed purchase intent, and build "lookalike audiences" that target users with similar behaviors or characteristics. These practices significantly improve advertising efficiency and increase the likelihood of converting user engagement into actual sales.

60. Data harvesting is one of the fastest growing industries in the country, with estimates suggesting that internet companies earned $202 per American user in 2018 from mining and selling data. That figure is expected to increase with estimates for 2022 as high as $434 per use, reflecting a more than $200 billion industry.

61. Defendant has a strong financial incentive to deploy the Trackers on its Website without obtaining user consent. By enabling the collection of IP addresses and device-level identifiers through these technologies, Defendant facilitates integration into real-time bidding ecosystems. These systems rely on bidstream data—such as IP address, device type, screen resolution, and referral information—to assess the value of a potential ad impression. This enables Defendant and its partners to participate in data-driven ad targeting, increase the value of its advertising inventory, and track users across sessions and websites, all of which provide economic benefit despite private implications to users.

62. IP addresses are a valuable data point in digital advertising and tracking systems. They can be used to approximate a user's geographic location, often down to the city or ZIP code level, enabling location-based targeting. When combined with cookies, browser metadata, and device identifiers, IP addresses contribute to persistent user tracking across sessions and websites. They also assist advertisers and data brokers in linking anonymous browsing activity to existing user profiles, which enhances ad targeting precision and increases the commercial value of each tracked interaction. IP

addresses therefore constitute "routing, addressing, or signaling information" protected under CIPA § 638.50(b).

63. When users' data is collected without meaningful consent and monetized, they lose control over who can access, use, or distribute their personal information. Data brokers and ad tech firms aggregate and correlate identifiers—such as IP addresses, device IDs, and cookies—with other personal data to construct detailed consumer profiles. Information initially gathered in one context, such as browsing a retail website, is frequently repurposed for unrelated uses and sold to third parties without the user's awareness. This results in pervasive surveillance, where users are continuously tracked across multiple websites, applications, and devices, often without their knowledge or ability to opt out.

6. *The Trackers Function Together to Achieve Targeted Objectives*

64. When a user visits the Website, a suite of background tracking technologies is activated immediately upon page load. These include client-side scripts deployed by third-party Trackers, which begin collecting various categories of User Information without any visible indication to the user. Together, these technologies function as a coordinated data collection infrastructure that allows Defendant to analyze user behavior at a highly granular level and to leverage that insight in real time for marketing optimization, user targeting, and business intelligence.

65. On information and belief, the Trackers operate as part of a vast and interconnected digital advertising ecosystem and these entities leverage shared identifiers, cookie syncing, and cross-device tracking techniques to follow users across websites, platforms, and environments, with tools specifically engineered to build persistent consumer profiles, enabling real-time behavioral targeting and identity resolution at scale.

66. On the Website, a coordinated network of third-party trackers is used to support the company's goals of identity resolution, targeted advertising, and data monetization. At the center of this system is Adobe Dynamic Tag Manager (DTM),

which acts as the command hub for deploying and managing other trackers. Adobe DTM is automatically triggered during the initial page load and executes JavaScript code that dynamically injects scripts from third parties such as Facebook, Google Ads, The Trade Desk, and others. This system enables the collection and distribution of user behavior data in real time—often before the user is presented with any consent interface.

67. Identity resolution on the site is primarily facilitated through the interplay of the Qualtrics tracker, Facebook Pixel, and AdRoll. Qualtrics silently monitors user behavior, even when no survey is active, and builds an internal behavioral profile. The Facebook Pixel identifies users by linking activity on truist.com to logged-in Facebook sessions or cookies, tying site interactions to social media profiles. AdRoll further enhances identity resolution by tracking users across websites and devices, using persistent IDs to stitch together behaviors from different sessions and platforms. This combination allows Truist to de-anonymize visitors over time, associate behaviors with identities, and build rich behavioral and demographic profiles.

68. Once identity signals are gathered, targeted advertising and data monetization are executed through Google Ads / DoubleClick, The Trade Desk, and Microsoft Ads. Google Ads and DoubleClick use this data to deliver personalized ads across Google's extensive ad networks, including search and display properties. The Trade Desk leverages programmatic ad exchanges to purchase targeted ad space in real time, allowing Truist to reach users across the broader internet with precision. Microsoft Ads fulfills a similar role within the Bing and LinkedIn ecosystems. Altogether, this system allows Truist to convert website traffic into measurable marketing outcomes, build and retarget high-value audiences, and ultimately monetize user engagement by driving conversions across its suite of financial services.

V. SPECIFIC ALLEGATIONS

1. The Adobe DTM Tracker

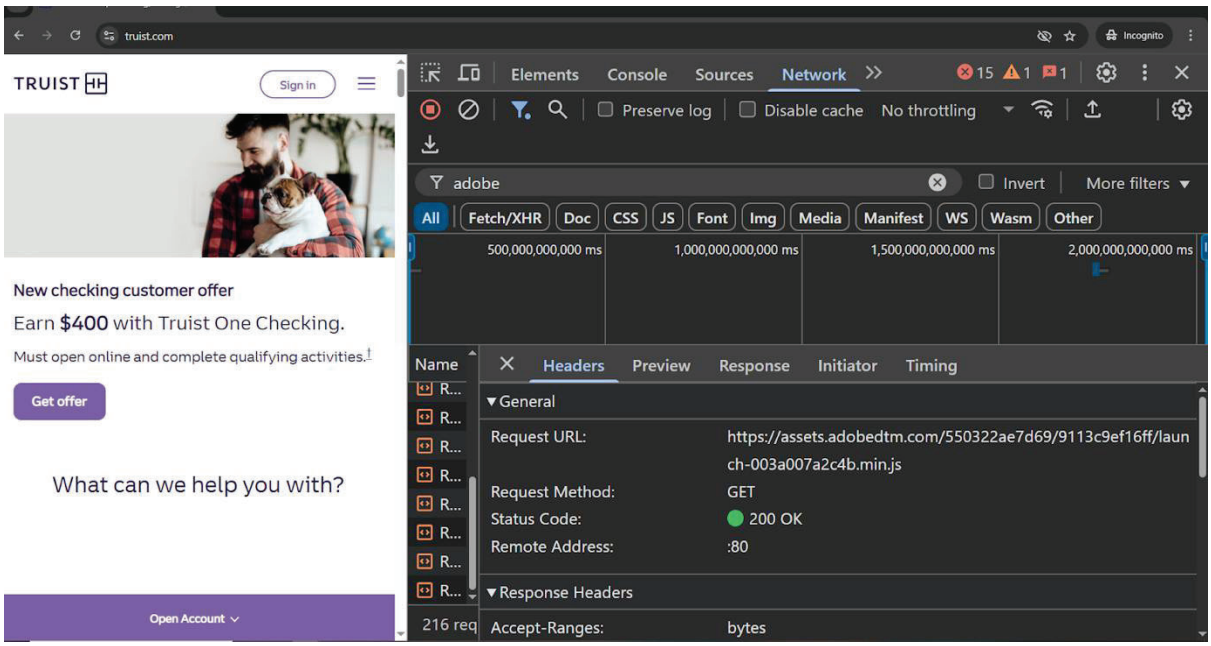
69. The Adobe DTM (Dynamic Tag Manager) tracker is a tag management system that enables the Website to dynamically load and manage third-party marketing

and analytics scripts. The tracker appears on the Website as a script loaded from assets.adobedtm.com. It acts as a central controller, firing other trackers such as Facebook Pixel, Google Ads, and Qualtrics based on user interactions like page views or clicks. By doing so, Adobe DTM facilitates real-time data collection and tracking across multiple vendors.

70. Adobe DTM listens for specific user actions—such as page views, button clicks, form submissions, or scroll events—and uses these triggers to fire other tracking tools. In doing so, it facilitates the collection of detailed behavioral data including navigation paths, engagement patterns, form field interactions, and device and/or browser information. Adobe DTM directly enables the tracking of sensitive signals such as login status, user IDs, and referrer URLs, which can be used for analytics, advertising, or identity resolution.

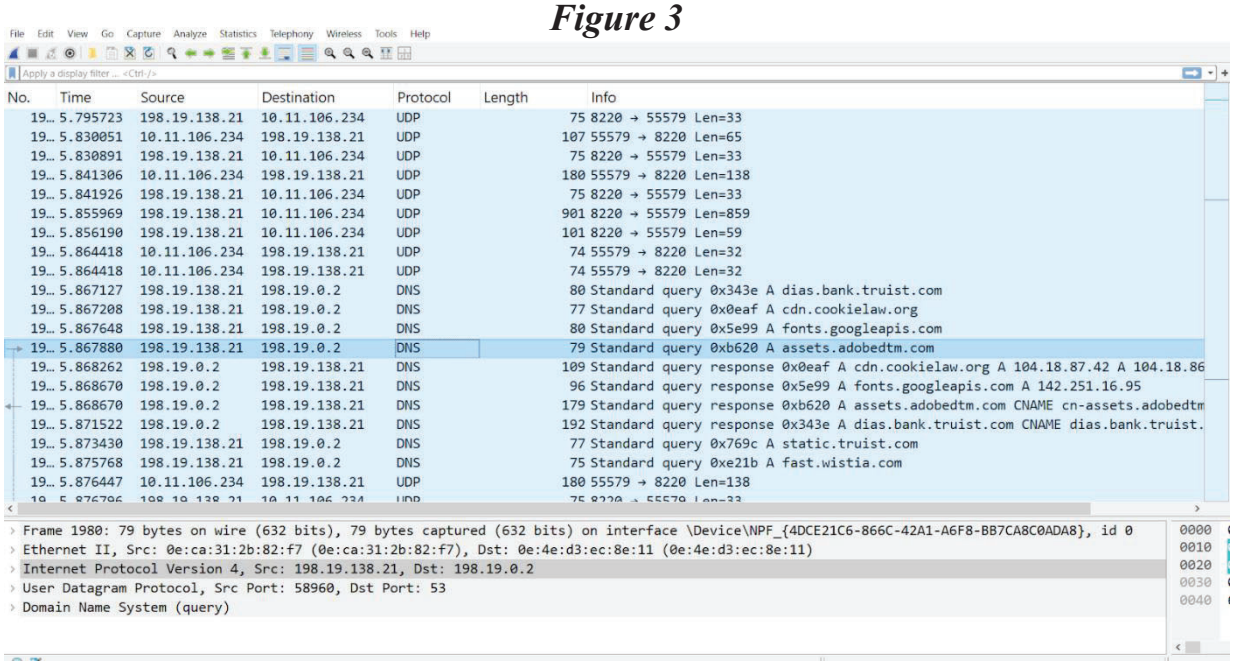
71. ***Figure 2*** below is a screenshot of the Website, which demonstrates that Adobe DTM (assets.adobedtm.com) was automatically loaded into the user's browser during the initial page load, without any direct user interaction:

Figure 2



72. ***Figure 3*** below is a screenshot of website activity on the Website, which shows that the user's browser initiated a DNS resolution request for the domain assets.adobedtm.com, indicating that the browser attempted to connect to Adobe's tag management infrastructure during the session. This confirms that the Adobe DTM tracker was loaded and active automatically upon page load, without any user interaction or opt-in consent:

Figure 3



73. The Adobe Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

74. The Adobe Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. See, e.g., James v. Walt Disney Co. 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

75. The Adobe DTM Tracker collects or enables the collection of outbound signaling data (like which URL the user is on, what links they clicked, and what form fields were interacted with), and often does so before any user consent is obtained, it closely mirrors the technical function of a pen register. Additionally, it may receive and process incoming data from servers in response to user behavior, aligning with the legal definition of a trap and trace device.

76. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' consent to install the Adobe Tracker or to collect or share data with Adobe.

77. Defendant's secret installation of the Adobe Tracker on the Website violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

2. The Qualtrics Tracker

78. The Qualtrics Tracker is a behavioral monitoring tool embedded on websites to support survey delivery, user experience research, and audience segmentation. On the Website, it appears through domains like siteintercept.qualtrics.com and iad1.qualtrics.com.

79. Even when no visible survey is displayed, the Qualtrics Tracker monitors user actions such as page views, time spent on site, navigation patterns, and clicks. This data is used to determine when and how to trigger surveys or intercepts and can also be integrated with advertising platforms for targeting and personalization.

80. The Qualtrics Tracker's data collection extends far beyond basic survey logic. It records user interactions such as button presses, form focus events, and navigation sequences, which are integrated with audience segmentation tools and advertising platforms.

81. ***Figure 4*** below is a screenshot from the Website, which demonstrates that the Qualtrics Tracker (siteintercept.qualtrics.com) was automatically loaded into the user's browser during the initial page load, without any direct user interaction:

//

//

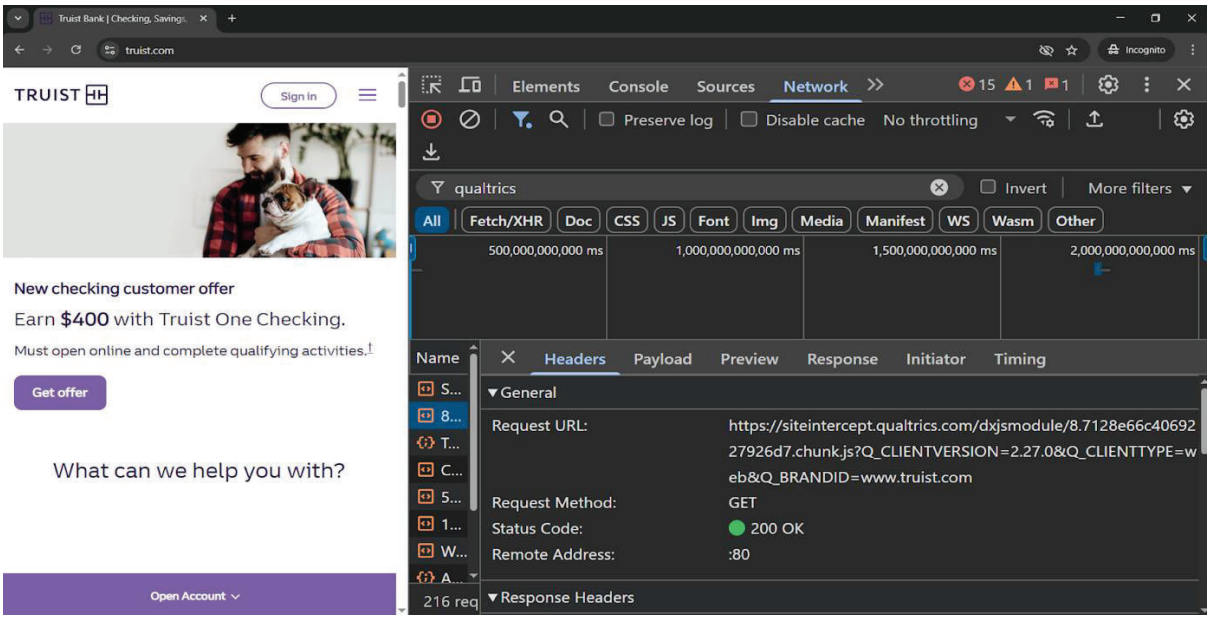
//

//

//

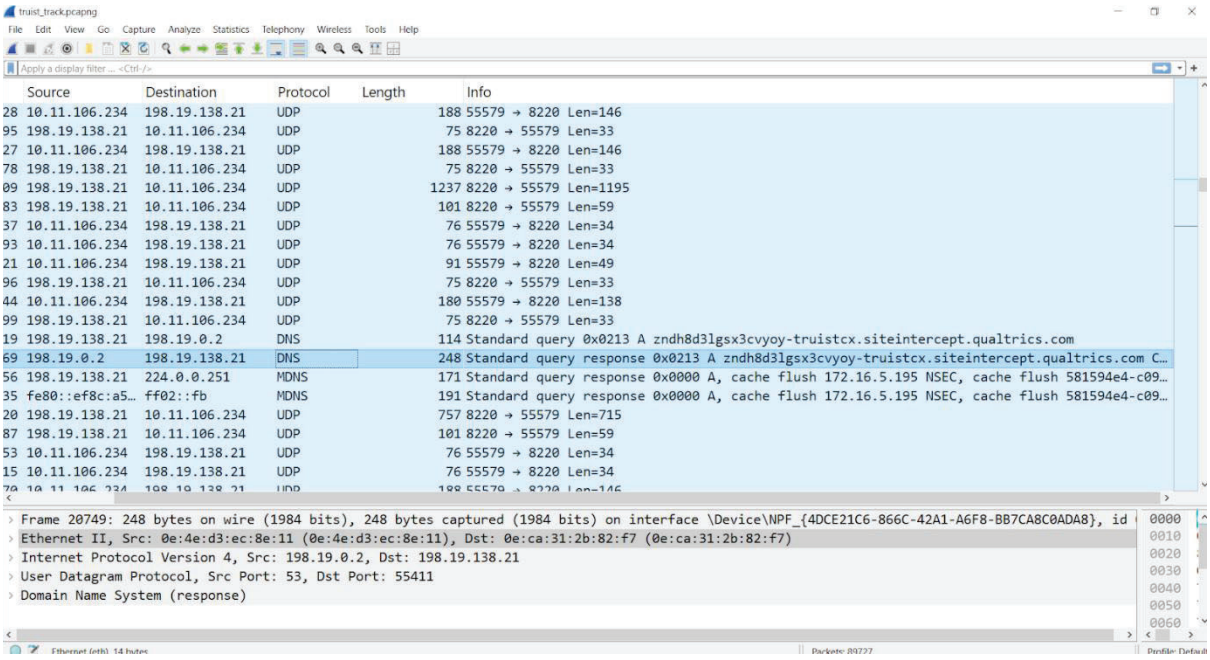
//

Figure 4



82. ***Figure 5*** below is a screenshot of web activity on the Website, which shows that the user's browser initiated a DNS resolution request for siteintercept.qualtrics.com, confirming that the Qualtrics Tracker was engaged automatically during the user session. This request demonstrates that tracking was initiated without any user action or visible prompt, indicating passive surveillance functionality:

Figure 5



83. The Qualtrics Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

84. The Qualtrics Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. See, e.g., *James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

85. The Qualtrics Tracker functions as both a trap and trace device and a pen register because it silently intercepts and records signaling information during a user's interaction with the website. As a pen register, it captures outgoing signals such as the URLs visited, buttons clicked, form fields interacted with, and navigation paths—effectively logging the user's behavioral output. Simultaneously, it serves as a trap and trace device by processing incoming signals, such as data requests and server responses that help determine when to trigger surveys or data capture events.

86. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' consent to install the Qualtrics Tracker or to collect or share data with Qualtrics.

87. Defendant's secret installation of the Qualtrics Tracker on the Website violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

3. The Facebook Tracker

88. The Facebook Tracker is a behavioral tracking script employed via domains such as connect.facebook.net and facebook.com/tr/. On the Website, the Facebook Tracker is embedded through a JavaScript snippet and/or loaded dynamically through Google Tag Manager.

89. Once the user loads a page, the Facebook Tracker executes automatically, capturing information such as page views, button clicks, form interactions, and scroll behavior. These interactions are sent back to Meta's servers and associated with the

user's Facebook or Instagram profile — even if the user never directly interacts with Meta while on the Website.

90. The data collected by the Facebook Tracker supports identity resolution by linking behavioral data from the Website with individual user profiles across Meta's platforms. If the user is logged into Facebook, Instagram, or Messenger on the same device or browser, the Meta Pixel can tie Website behavior to the user's unique Meta ID. This linkage allows Meta to build persistent, cross-site user profiles that include financial interest signals, such as engagement with mortgage tools, financial calculators, or account services. Even if the user is not logged in, Meta can assign a persistent identifier via first- and third-party cookies, pixel fires, or browser fingerprinting.

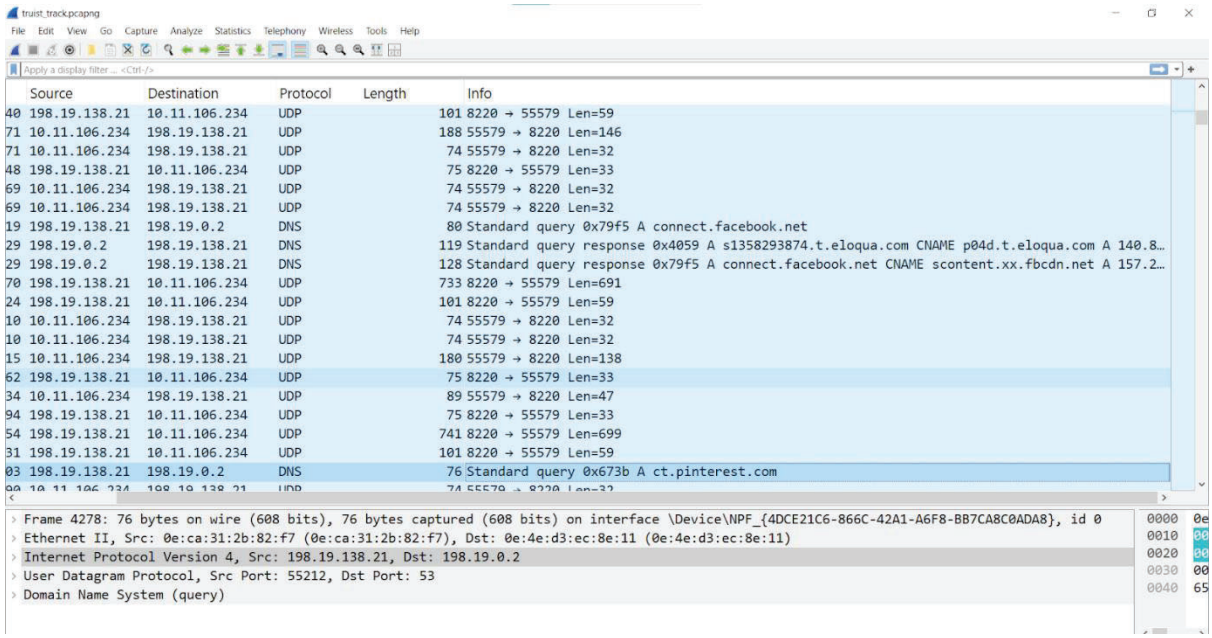
91. The Facebook Tracker also serves TRUIST's goal of targeted advertising by enabling the creation of "Custom Audiences" — groups of users who have taken specific actions on the Website, such as visiting the home equity loan page or starting an application. TRUIST can then use Facebook Ads Manager to re-target those users with ads across Facebook and Instagram, or use "Lookalike Audiences" to reach new users who exhibit similar online behavior. This cycle enables precise, cost-efficient delivery of BMO's advertising to consumers who are more likely to convert.

92. The Facebook Tracker contributes to TRUIST's data monetization strategy by turning behavioral insights into measurable advertising ROI. By tracking users across pages and sessions, Meta provides TRUIST with real-time analytics about user behavior, ad performance, and customer engagement. The Facebook Tracker closes the feedback loop between website behavior and ad delivery, allowing TRUIST to optimize ad spend, personalize messaging, and extract greater value from each visitor interaction. In this way, the Facebook Tracker functions as a critical part of TRUIST's commercial surveillance infrastructure, facilitating continuous behavioral profiling, identity matching, and monetization of user activity.

93. ***Figure 6*** below is a screenshot of Website activity, which confirms that the Facebook Tracker script was loaded upon page load, prior to user consent, triggering

communication with Meta's tracking infrastructure and the collection of user behavior data:

Figure 6



94. Defendant embedded the Facebook Tracker by inserting Meta's JavaScript pixel either directly into the Website's source code or through a tag manager like Google Tag Manager. Upon loading the page, the user's browser automatically executes this script, triggering communication with Meta's servers and transmitting metadata such as the user's IP address, page URL, and browser details. This occurs without any user engagement, making the tracking behavior silent and involuntary from the user's perspective.

95. The Facebook Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

96. The Facebook Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. *See*, e.g., *James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

97. The Facebook Tracker captures and transmits routing, addressing, and signaling information — such as the user's IP address, page URL, referrer, and browser metadata — to Meta's servers the moment a page loads, often without the user's

knowledge or consent. This type of metadata identifies the origin and destination of an electronic communication. Critically, the user is not attempting to communicate with Facebook; the connection is silently triggered by code embedded in the website, enabling Meta to intercept and persistently associate the user's behavioral signals with a known or inferred identity, enabling commercial surveillance through passive third-party data collection.

98. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' express or implied consent to install the Facebook Tracker on Plaintiff's and Class Members' browser or to collect or share data with Facebook.

99. Consequently, the Facebook Tracker violates CIPA regarding unauthorized use of a pen register without prior consent or court order.

4. The Google Ads / DoubleClick Tracker

100. Google Ads and DoubleClick are digital advertising technologies owned and operated by Google LLC. Google Ads powers paid advertisements on Google's own properties (such as Google Search and YouTube) as well as across its partner network. DoubleClick—now part of Google Marketing Platform—specializes in display and programmatic advertising, enabling real-time ad bidding and behavioral targeting across millions of third-party websites.

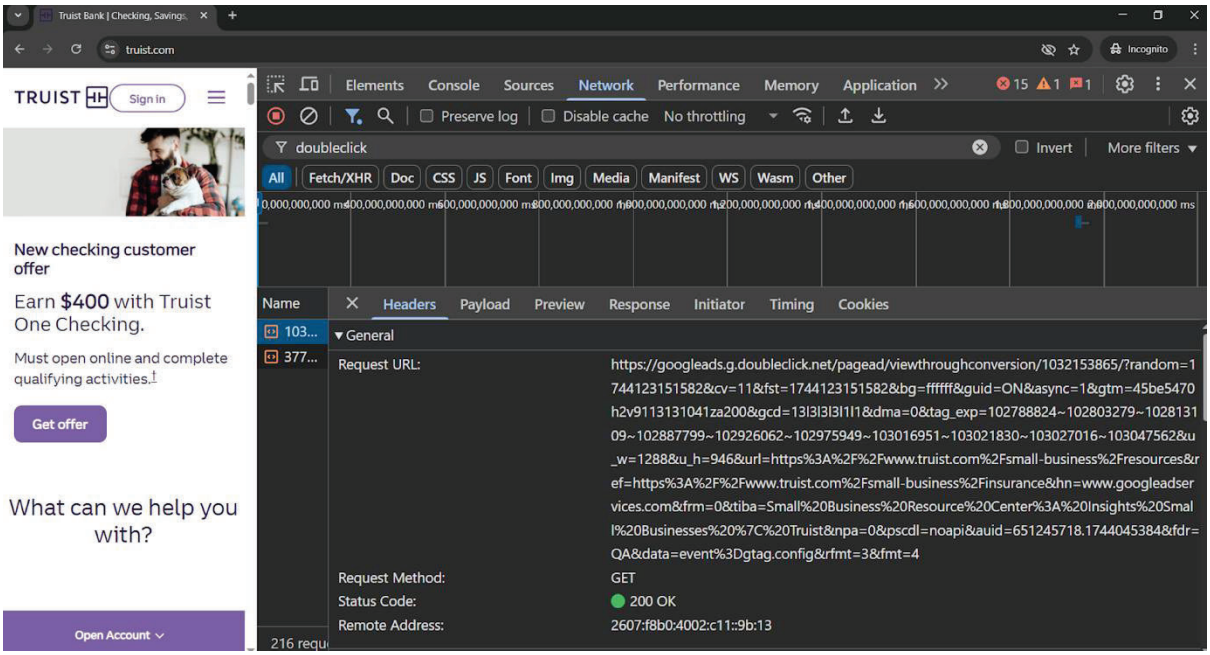
101. When implemented on the Website, these tools track a wide array of user signaling information. This includes the URLs visited, time spent on pages, links clicked, and referrer data (i.e., where a visitor came from). They also collect device and browser details, including IP address, operating system, screen size, and location estimates. Through browser cookies and pixel tags, Google can assign users unique identifiers that allow tracking across different sessions, websites, and even devices. These identifiers are linked to user profiles, which may include inferred interests (e.g., finance, travel, parenting) based on prior web activity.

//

102. Both Google Ads and DoubleClick monitor conversion events, such as form submissions, purchases, or account sign-ups. This allows advertisers—including companies like TRUIST—to measure the effectiveness of campaigns and optimize ad delivery. The data is used not just for analytics, but also for building custom audiences and lookalike audiences, enabling highly targeted advertising across the web. These trackers are embedded via scripts like googleads.g.doubleclick.net or adservice.google.com and are triggered without user interaction.

103. ***Figure 7*** below is a screenshot from the Website, which demonstrates that the DoubleClick Tracker (googleads.g.doubleclick.net) was automatically loaded into the user's browser during the initial page load, without any direct user interaction:

Figure 7

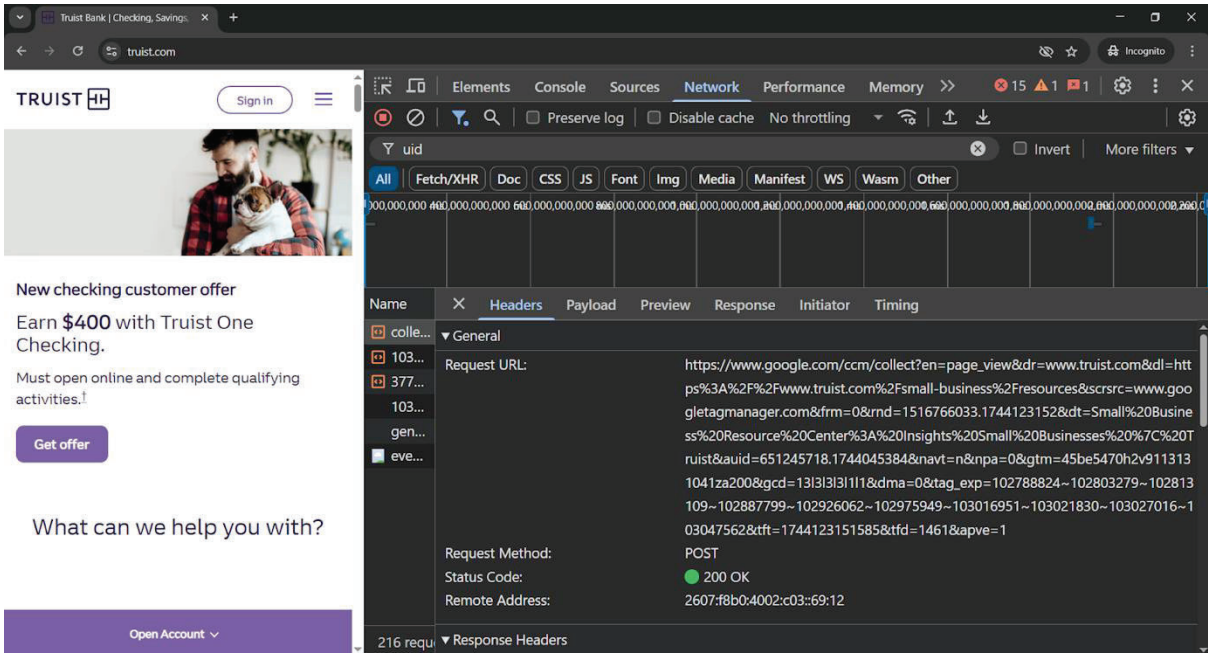


104. ***Figure 8*** below is a screenshot from the Website, which demonstrates that the Google Ads Tracker (googleads.g.doubleclick.net) was activated with a unique User ID:

//

//

Figure 8



105. Defendant surreptitiously installed, executed, embedded or injected the Google Ads / DoubleClick Tracker onto users' browsers by copying the JavaScript code snippet and adding it to the Website. When a user visits the Website, their browser executes the JavaScript code which sends data about the user's interactions, including the user's IP address, to Google's servers as part of third-party tracking and advertising infrastructure.

106. The Google Ads / DoubleClick Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

107. The Google Ads / DoubleClick Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. *See*, e.g., *James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

108. The Google Ads and DoubleClick trackers operate as both pen registers and trap and trace devices under CIPA because they capture outgoing signaling data—such as URLs visited, click paths, session timestamps, and form activity—and also process incoming data like ad impressions and pixel loads. These trackers are activated passively during page load and function without any direct user

request, enabling real-time transmission of communication metadata to Google's advertising infrastructure.

109. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' express or implied consent to install the Google Ads / DoubleClick Tracker on Plaintiff's and Class Members' browser or to collect or share data with Google.

110. Consequently, the Google Ads / DoubleClick Tracker violates CIPA regarding unauthorized use of a pen register without prior consent or court order.

5. The AdRoll Tracker

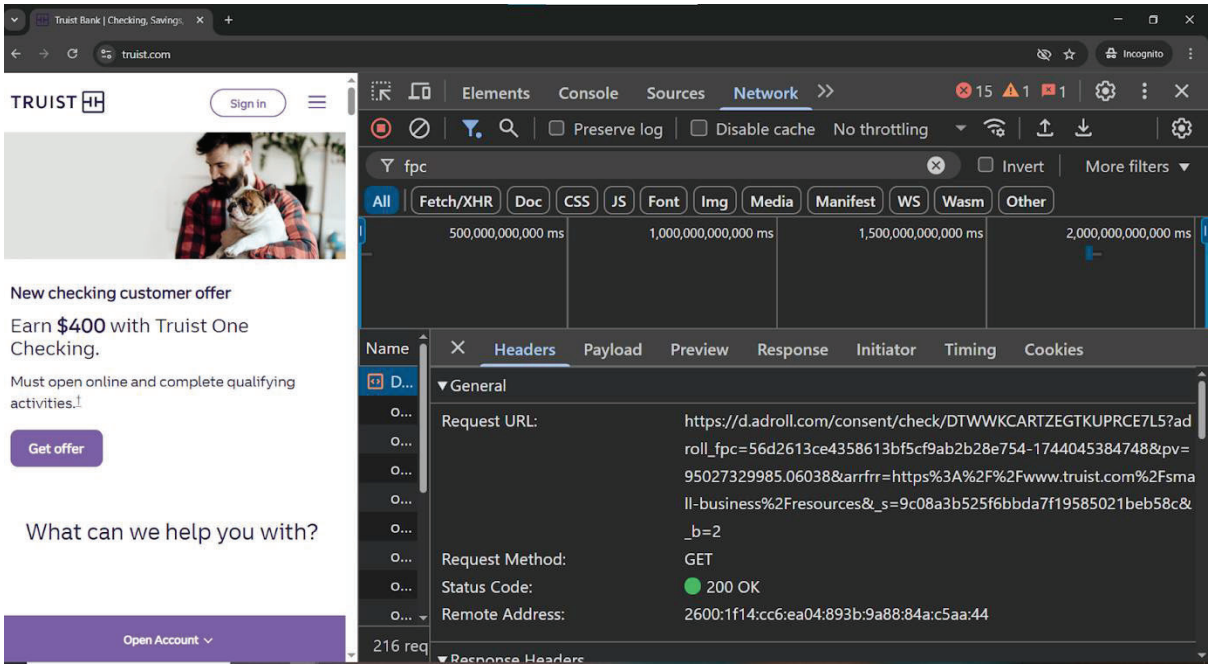
111. The AdRoll Tracker, typically served from the domain d.adroll.com, is a behavioral advertising pixel owned and operated by NextRoll, Inc. (formerly AdRoll, Inc.). It is a cross-site tracking technology designed to monitor users' online activity and serve personalized, retargeted advertisements based on individual behavior.

112. The AdRoll Tracker records detailed user behavior on the Website, including pages visited, time spent, product views, clicks, and abandonments. This data is analyzed to create behavioral segments (e.g., "home loan interest," "wealth management prospects," etc.). These segments are then used to display personalized ads to the same users across thousands of third-party websites, including news outlets, retail sites, and social media.

113. The AdRoll Tracker is designed to utilize device fingerprinting, cookie syncing, and hashed email matching to persistently identify users across devices and sessions. Through programmatic ad exchanges, the AdRoll Tracker enables Defendant to participate in real-time auctions for ad impressions, using the behavioral data collected to bid higher for users deemed more valuable.

114. Defendant installed, executed, embedded, or injected the AdRoll Tracker onto users' browsers. ***Figure 9*** below is a screenshot of the Website, which documents the parameter adroll_fpc seen in a GET request to d.adroll.com containing tracking values:

Figure 9



115. The AdRoll Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

116. The AdRoll Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. *See*, e.g., *James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

117. The AdRoll Tracker initiates a connection to its parent company's servers (typically at d.adroll.com) upon page load or user interaction. This connection sends routing and signaling metadata including IP address, user-agent string, full URL path, referrer header, and timestamp—all of which help identify the source and destination of the communication.

118. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' consent to install the AdRoll Tracker or to collect or share data with NextRoll, Inc.

/ /

/ /

119. Defendant's secret installation of the AdRoll Tracker on the Website violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

6. The Trade Desk Tracker

120. The Trade Desk Tracker, typically delivered via the domain adsrvr.org, is a third-party behavioral tracking pixel. On the BMO website, this tracker is either embedded directly or injected dynamically through a tag management system. When a user visits the site, the tracker initiates a connection to The Trade Desk's servers, capturing a range of data points including IP address, device type, browser version, geolocation, and unique cookie or device identifiers. These interactions confirm that the user's activity is being observed and recorded for later use in digital advertising campaigns.

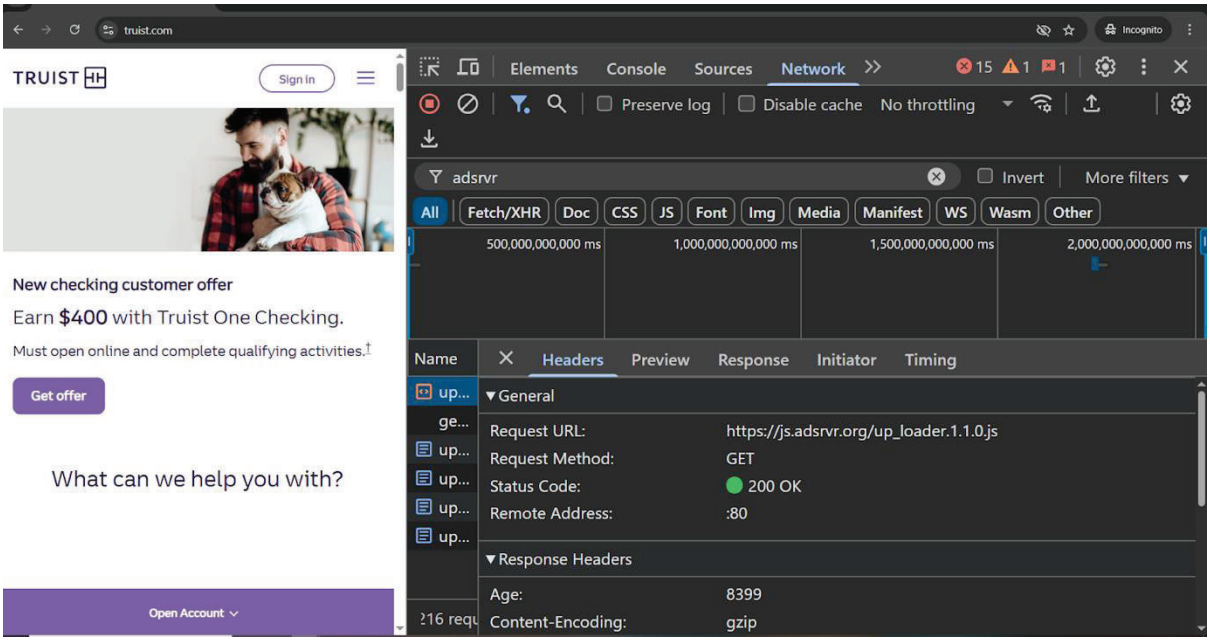
121. Once activated, the Trade Desk Tracker plays a central role in identity resolution by assigning users a persistent identifier that can be recognized across other websites, apps, and devices. This is accomplished through techniques such as cookie syncing, hashed email matching, and participation in the Trade Desk's Unified ID 2.0 (UID2) system — an identity framework designed to replace third-party cookies. These tools allow The Trade Desk to connect behavioral data collected on BMO's site with broader user profiles across the internet, creating a cohesive view of an individual's online behavior even when they are not logged in.

122. In terms of targeted advertising, the Trade Desk Tracker enables TRUIST to reach users who previously visited the Website, viewed financial products, or began applications — through retargeting ads served across thousands of partner websites and ad exchanges. The Trade Desk Tracker's data enrichment tools allow TRUIST to identify behavioral traits and interests among their site visitors, and then build lookalike audiences composed of similar users for future ad campaigns. This significantly enhances TRUIST's ability to reach new but relevant users who are likely to be interested in its financial services.

123. The Trade Desk Tracker supports TRUIST's broader objective of data monetization by transforming real-time behavioral signals into actionable, revenue-generating insights. By tracking users across multiple touchpoints and matching them to advertising segments, TRUIST gains access to detailed performance analytics and the ability to optimize ad spend. The data collected feeds into a programmatic ad-buying ecosystem where advertisers compete to show personalized ads to high-value users — often based on the very behavioral traits observed on TRUIST's site. In this way, The Trade Desk enables TRUIST to extract commercial value from user activity, while facilitating profiling and ad delivery practices.=

124. ***Figure 10*** below is a screenshot of the website activity on the Website, which shows that the user's browser initiated a DNS resolution request for js.adsrvr.org, the domain associated with The Trade Desk's tracker. This request occurred during the initial session load, confirming that tracking infrastructure was contacted automatically, without any intentional user communication or interaction:

Figure 10

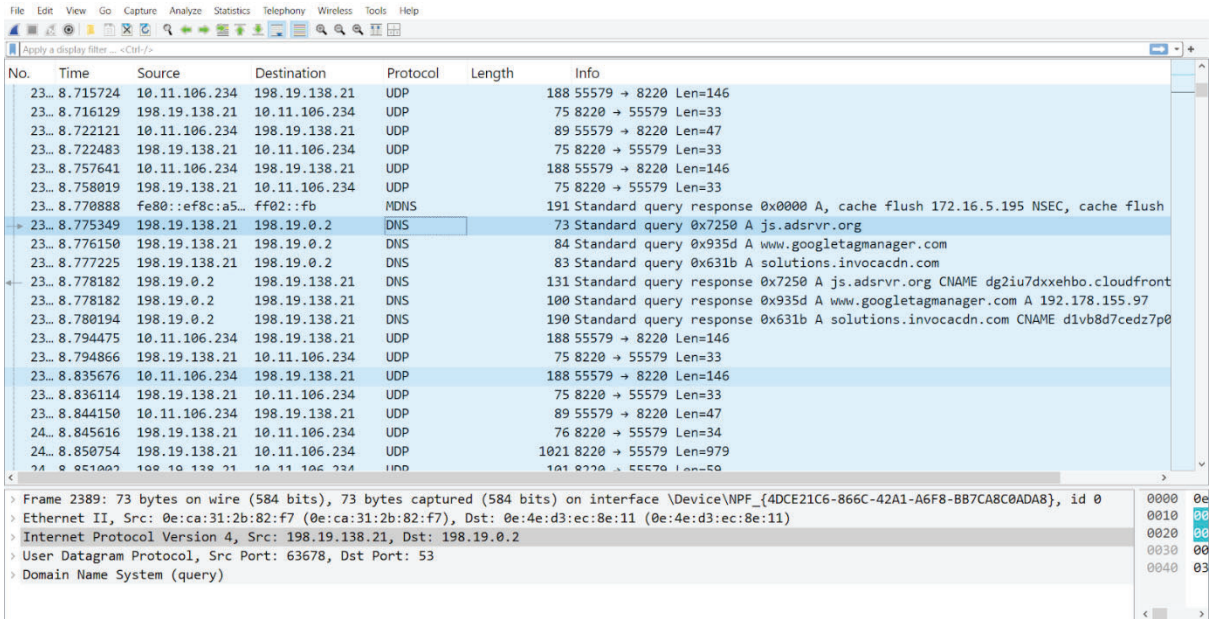


/ /

/ /

125. ***Figure 11*** below is a screenshot of website activity on the Website, which reflects a DNS request that confirms that The Trade Desk tracker was operational during the session, and that the browser was actively attempting to transmit routing and signaling metadata to Trade Desk's third-party server:

Figure 11



126. Defendant surreptitiously installed, executed, embedded or injected The Trade Desk Tracker onto users' browsers by copying the JavaScript code snippet and adding it to the Website. When a user visits the Website, their browser executes the JavaScript code which sends data about the user's interactions, including the user's IP address, to Trade Desk's servers.

127. The Trade Desk Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

128. The Trade Desk Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. See, e.g., *James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

129. The Trade Desk Tracker initiates a connection to its ad infrastructure upon page load via a script or pixel execution. It captures user metadata such as IP

address, page path, timestamp, and unique identifiers — all of which qualify as routing or signaling information under CIPA.

130. The user is not intentionally initiating any communication with The Trade Desk; rather, the connection is automatically triggered in the background by embedded third-party code. As a result, The Trade Desk is able to silently intercept, and log communication-related data generated during the user's interaction with the Website. In this way, the Trade Desk Tracker functions as a surveillance mechanism that captures third-party signaling information.

131. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' express or implied consent to install The Trade Desk Tracker on Plaintiff's and Class Members' browser or to collect or share data with The Trade Desk.

132. Consequently, The Trade Desk Tracker violates CIPA regarding unauthorized use of a pen register without prior consent or court order.

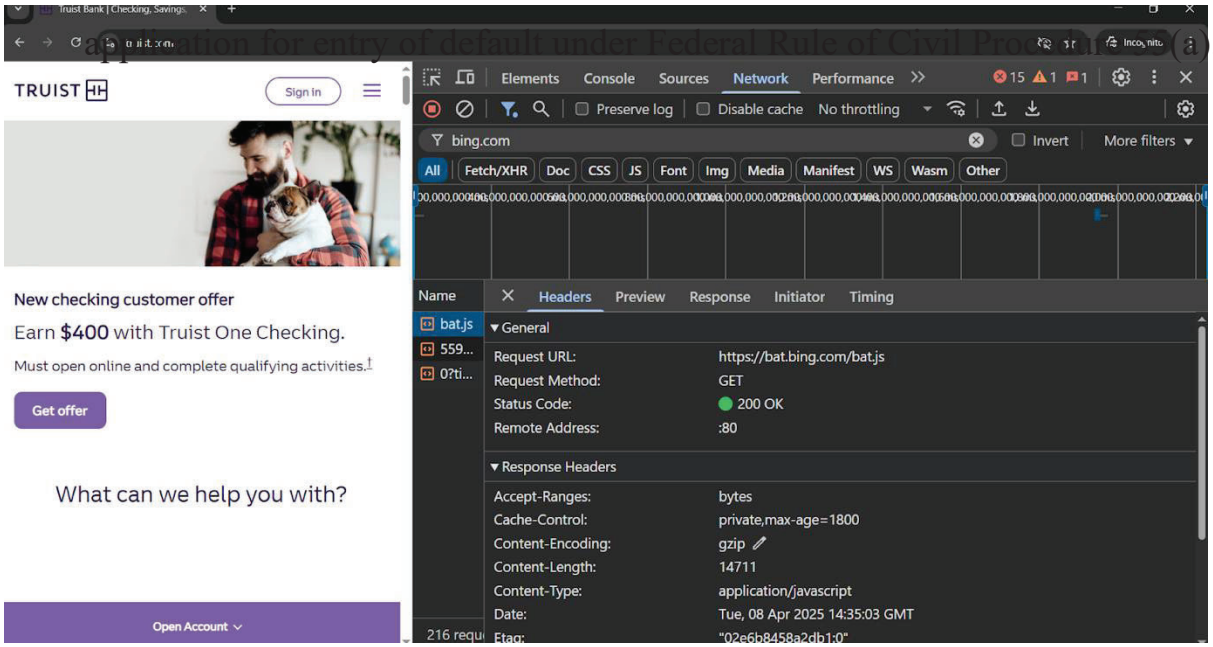
7. The Microsoft Ads Tracker

133. The Microsoft Ads Tracker—typically delivered through the domain bat.bing.com—is part of the Microsoft Advertising platform (formerly Bing Ads). It is used to track user interactions on websites in order to attribute conversions, retarget visitors, and optimize advertising campaigns across Microsoft's search and display networks, including Bing, MSN, and LinkedIn.

134. When a user visits the Website, the Microsoft Ads Tracker silently collects a range of data including the pages viewed, click events, referrer URL, and conversion actions (e.g., form submissions or account sign-ups). It also gathers device and browser information, IP address, and estimated geolocation. Through the use of cookies and unique identifiers, Microsoft Ads can follow users across sessions and websites to build behavioral profiles and serve targeted ads.

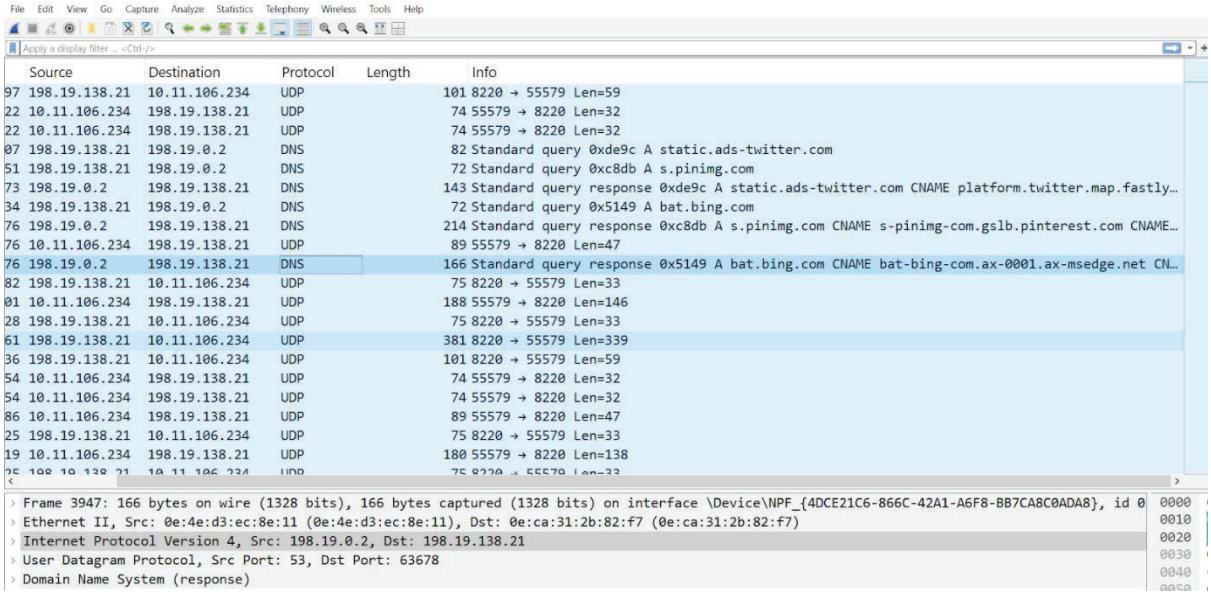
135. ***Figure 12*** below is a screenshot from the Website, which shows that the Microsoft Ads Tracker loaded automatically on the user's browser:

Figure 12



136. ***Figure 13*** below is a screenshot of website activity on the Website, which shows that the user's browser initiated and completed a DNS resolution request for the domain bat.bing.com, confirming that the Microsoft Ads Tracker was activated during the user's session. This activity illustrates an attempt to connect to Microsoft's ad delivery and tracking infrastructure without any direct user action:

Figure 13



137. Defendant surreptitiously installed, executed, embedded or injected the Microsoft Ads Tracker onto users' browsers by copying the JavaScript code snippet and adding it to the Website. When a user visits the Website, their browser executes the JavaScript code which sends data about the user's interactions, including the user's IP address, to Microsoft's servers.

138. The Microsoft Ads Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

139. The Microsoft Ads Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. See, e.g., *James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

140. The Microsoft Ads Tracker initiates a connection to its ad infrastructure upon page load via a script or pixel execution. It captures user metadata such as IP address, page path, timestamp, and unique identifiers - all of which qualify as routing or signaling information under CIPA.

141. The Microsoft Ads Tracker collects real-time signaling and routing information from the user's device without direct interaction. It acts as a pen register by capturing outbound metadata such as page visits, click events, and form submissions, and as a trap and trace device by receiving inbound responses like ad content and tracking pixels. These communications occur passively, enabling Microsoft to assign user identifiers, build behavior profiles, and facilitate personalized advertising—all without the user's knowledge or consent.

142. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' express or implied consent to install the Microsoft Ads Tracker on Plaintiff's and Class Members' browser or to collect or share data with Microsoft.

143. Consequently, the Microsoft Ads Tracker violates CIPA regarding unauthorized use of a pen register without prior consent or court order.

//

VI. CLASS ALLEGATIONS

144. Plaintiff brings this action individually and on behalf of all others similarly situated (the "Class" or "Class Members") defined as follows:

> All persons within California on whose browser Defendant installed, executed, embedded or injected the Trackers without a court order or consent within the statute of limitations period.

145. **NUMEROSITY:** Plaintiff does not know the number of Class Members but believes the number to be in the thousands, if not more. The exact identities of Class Members can be ascertained by the records maintained by Defendant.

146. **COMMONALITY:** Common questions of fact and law exist as to all Class Members and predominate over any questions affecting only individual members of the Class. Such common legal and factual questions, which do not vary between Class members, and which may be determined without reference to the individual circumstances of any Class Member, include but are not limited to the following:

- Whether Defendant installed, executed, embedded or injected the Trackers on the Website;
- Whether the Trackers are each a pen register and/or trap and trace device as defined by law;
- Whether Plaintiff and Class Members are subject to same tracking policies and practices;
- Whether Plaintiff and Class Members are entitled to statutory penalties;
- Whether Class Members are entitled to injunctive relief;
- Whether Class Members are entitled to disgorgement of data unlawfully obtained;
- Whether the Defendant's conduct violates the California Constitution;
- Whether the Defendant's conduct constitutes an intrusion upon seclusion;
- Whether the Defendant's conduct violates the Cal. Civil Code §

1178.100, *et seq.;*

- Whether the Defendant's conduct constitutes an unlawful, misleading, deceptive or fraudulent business practice; and
- Whether Plaintiff and the Class Members are entitled to equitable relief for unjust enrichment.

147. **TYPICALITY:** As a person who visited Defendant's Website and whose outgoing electronic information was surreptitiously collected by the Trackers, Plaintiff is asserting claims that are typical of the Class Members. Plaintiff's experience with the Trackers is typical to Class Members.

148. **ADEQUACY:** Plaintiff will fairly and adequately protect the interests of the members of the Class. Plaintiff has retained attorneys experienced in class action litigation. All individuals with interests that are actually or potentially adverse to or in conflict with the Class or whose inclusion would otherwise be improper are excluded.

149. **SUPERIORITY:** A class action is superior to other available methods of adjudication because individual litigation of the claims of all Class Members is impracticable and inefficient. Even if every Class Member could afford individual litigation, the court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed.

VII. FIRST CAUSE OF ACTION

Violations of Cal. Penal Code § 638.51

By Plaintiff Against All Defendants

150. Plaintiff reasserts and incorporates by reference the allegations set forth in each preceding paragraph as though fully set forth herein.

151. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

152. Defendant uses a pen register device or process and/or a trap and trace device or process on its Website by deploying the Trackers because the Trackers are designed to capture the IP address, User Information and other information such as the

phone number, email, routing, addressing and/or other signaling information of website visitors.

153. Defendant did not obtain consent from Plaintiff or any of the Class Members before using pen registers or trap and trace devices to locate or identify users of its Website and has thus violated CIPA. CIPA imposes civil liability and statutory penalties for violations of § 638.51. Cal. Penal Code § 637.2; *Moody v. C2 Educational Systems, Inc.*, No. 2:24-cv-04249-RGK-SK, 2024 U.S. Dist. LEXIS 132614 (C.D. Cal. July 25, 2024).

VIII. SECOND CAUSE OF ACTION

Violations of Cal. Constitution Article I § 1

By Plaintiff Against All Defendants

154. Plaintiff reasserts and incorporates by reference the allegations set forth in each preceding paragraph as though fully set forth herein.

155. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

156. Article I, Section 1 of the California Constitution guarantees each individual an inalienable right to privacy. This constitutional provision supports a private right of action against both governmental and private actors who engage in conduct that constitutes a serious invasion of privacy.

157. Plaintiff and the Class Members possess a legally protected privacy interest in the confidentiality of their online behavior, communications metadata, and identifying information, including but not limited to: IP address, browser details, session identifiers, page visit patterns, and clickstream behavior.

158. Plaintiff and the Class Members had a reasonable expectation that their activity on Defendant's website—including what pages were visited, what content was interacted with, and when—would not be secretly tracked and transmitted to third parties via embedded surveillance code.

159. Without Plaintiff's or the Class Members' knowledge or consent,

Defendant caused the Trackers to be deployed on the Website. The Trackers secretly transmitted Plaintiff's digital signaling data, addressing information (e.g., URLs accessed), and routing metadata (e.g., timestamps and referral paths) to the Third Parties, enabling behavioral profiling and cross-site identification.

160. Defendant's conduct constitutes a serious and egregious invasion of Plaintiff's and the Class Members' informational privacy, far exceeding any routine or incidental data handling. The deployment of real-time surveillance tools designed to accomplish identity resolution and behavioral mapping is highly offensive to a reasonable person.

161. Defendant lacked any legitimate justification for failing to disclose or obtain consent for this data interception and transfer. The magnitude of the privacy intrusion outweighed any speculative or commercial benefit to Defendant.

162. As a direct and proximate result of Defendant's actions, Plaintiff and the Class Members have suffered a loss of control over personal data, emotional distress, and a violation of their constitutional right to privacy.

IX. THIRD CAUSE OF ACTION

Violations of Cal. Civil Code § 1798.100, *et seq.*

By Plaintiff Against All Defendants

163. Plaintiff realleges and incorporates by reference all preceding paragraphs of this Complaint as though fully set forth herein.

164. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

165. The CCPA grants consumers legal rights subject to statutory protection, including the right to know what personal information is being collected about them and whether that information is sold or disclosed and to whom, the right to prohibit the sale of their personal information, the right to request deletion of their personal information, and the right to nondiscrimination in service and price when they exercise privacy rights. Ca. Civil Code § 1798.100 *et seq*.

166. The CCPA defines "personal information" broadly to include "...information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civil Code § 1798.140.

167. The CCPA dictates specifically that "[a] third party shall not sell or share personal information about a consumer that has been sold to, or shared with, the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out." Cal. Civil Code § 1798.115.

168. Defendant collected Plaintiff's and Class Members' personal information with the purpose of resolving their identities and locating them for targeted marketing in the course of and as part of its business with California consumers.

169. Disclosing Plaintiff's and Class Members' personal information was not reasonably necessary or proportionate to perform Defendant's reasonably expected online services.

170. By collecting, using, and/or selling Plaintiff's and Class Members' personal information and location data to Third Parties without providing sufficient notice, Defendant violated CCPA.

171. By failing to inform Plaintiff and Class Members of the personal information collected about them and that their personal information was shared with the Third Parties, Defendant violated CCPA.

X. FOURTH CAUSE OF ACTION

Violations of Business & Professions Code § 17200

By Plaintiff Against All Defendants

172. Plaintiff realleges and incorporates by reference all preceding paragraphs of this Complaint as though fully set forth herein.

173. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

174. This cause of action is brought under California Business & Professions

Code § 17200 et seq., which prohibits any unlawful, unfair, or fraudulent business act or practice.

175. Defendant has engaged in unlawful business practices by:

(a) Violating Article I, Section 1 of the California Constitution, which protects individuals from serious invasions of privacy;

(b) Violating California Penal Code §§ 638.50–638.56, including the unauthorized collection of addressing, signaling, and routing information for user identification and tracking; and

(c) Violating California Civil Code § 1798.100, *et seq.*, including collecting, using, and/or selling Plaintiff's and Class Members' personal information and location data to Third Parties without providing sufficient notice. Privacy rights rooted in the CCPA are a protected interest enforceable under Business & Professions Code § 17200. *Briskin v. Shopify, Inc*., 101 F.4th 706 (9th Cir. 2025) (en banc).

176. Defendant has engaged in unfair business practices by embedding the Trackers into the Website and enabling the real-time capture and transmission of Plaintiff's and Class Members' personal and behavioral information, such as IP address, browser details, visited URLs, referrer paths, timestamps, and interaction events, to the Third Parties.

177. The Defendant's practices are contrary to public policy supporting consumer privacy and data autonomy, and the harm it causes to consumers, including loss of control over personal information and risk of profiling, outweighs any legitimate business justification.

178. Defendant has engaged in fraudulent business practices by failing to adequately disclose its data-sharing practices. On information and belief, Defendant omitted material facts from its privacy policy and/or site interface and failed to inform users that their activities would be tracked across the internet and linked to unique identifiers for advertising and profiling purposes. These omissions were likely to deceive a reasonable consumer and were intended to obscure the nature and extent of

the surveillance.

179. As a direct and proximate result of Defendant's unlawful, unfair, and fraudulent conduct, Plaintiff and the Class Members have suffered injury in fact and loss of money or property, including the unauthorized exfiltration and commodification of valuable personal data. Plaintiff's and Class Members' data—used for targeted advertising, behavioral modeling, and enrichment by third parties—constitutes digital property with measurable economic value.

180. Plaintiff on behalf of himself and on behalf of the Class Members seeks injunctive relief to prevent Defendant from continuing its deceptive and unlawful data tracking practices and to require clear and conspicuous notice and opt-in consent for any behavioral tracking involving third-party tools. Plaintiff on behalf of himself and on behalf of the Class Members, also seeks restitution of the value derived from the unauthorized use of their personal information, attorneys' fees where permitted by law, and such other and further relief as the Court may deem just and proper.

XI. FIFTH CAUSE OF ACTION

Intrusion Upon Seclusion

By Plaintiff Against All Defendants

181. Plaintiff realleges and incorporates by reference all preceding paragraphs of this Complaint as though fully set forth herein.

182. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

183. Plaintiff and the Class Members bring this cause of action for intrusion upon seclusion, a well-established common law tort recognized in California, which protects individuals from intentional invasions of their private affairs in a manner that would be highly offensive to a reasonable person.

184. At all relevant times, Plaintiff and the Class Members had a reasonable expectation of privacy in their online browsing activity, including their interactions with the Website, the specific content viewed, and the behavioral signals generated through

use of the website—such as page views, click paths, session timestamps, and form entries.

185. Without Plaintiff's or Class Members' knowledge or consent, Defendant intentionally deployed the Trackers on the Website. This tool was engineered to surreptitiously capture and transmit granular behavioral data—including addressing, signaling, and routing information such as IP addresses, URL paths, referrers, device attributes, and mouse activity—to third parties.

186. The data collected was detailed and persistent, enabling Third Parties to monitor Plaintiff's and Class Members' conduct across websites, associate that behavior with unique identifiers, and build a behavioral profile of Plaintiff and Class Members for marketing and data monetization purposes.

187. Defendant's actions were intentional, systematic, and designed to operate in a manner undetectable by users. At no point did Defendant provide clear, conspicuous disclosure of this surveillance, nor did it obtain affirmative consent from Plaintiff and Class Members to conduct such monitoring or transmit the collected data to third parties.

188. The nature of this covert surveillance—especially its capacity to link online activity to identifiable users—would be highly offensive to a reasonable person, particularly in light of growing public sensitivity to privacy rights and digital surveillance.

189. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class Members suffered an invasion of privacy, loss of control over personal information, and emotional harm, including anxiety, indignity, and concern over being unknowingly tracked, profiled, and exposed to targeted advertising based on private digital conduct.

190. Defendant's conduct was willful, malicious, and oppressive, thereby justifying the imposition of punitive and exemplary damages.

/ /

XII. SIXTH CAUSE OF ACTION

Unjust Enrichment

By Plaintiff Against All Defendants

191. Plaintiff realleges and incorporates by reference all preceding paragraphs of this Complaint as though fully set forth herein.

192. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

193. Plaintiff and Class Members bring this cause of action for unjust enrichment, asserting that Defendant has been unjustly enriched through the unauthorized and uncompensated acquisition, use, and monetization of Plaintiff's and Class Members' personal data.

194. Plaintiff and the Class Members, while visiting and interacting with the Website, unknowingly conferred a substantial benefit on Defendant by generating digital behavioral data, including but not limited to IP address, device information, browser metadata, URL paths, session timestamps, and interaction signals.

195. Defendant deployed the Trackers without Plaintiff's and Class Members' knowledge or meaningful consent. The data collected was then used by Defendant and/or third parties to conduct behavioral targeting, analytics, and advertising optimization that generated substantial financial value.

196. At no time did Plaintiff and Class Members consent to the commercial exploitation of this data. Nor were Plaintiff and Class Members informed that their online behavior would be tracked and monetized in this manner. Plaintiff and Class Members received no compensation, disclosure, or opportunity to prevent the enrichment conferred upon Defendant.

197. Defendant's retention and use of this benefit was unjust and inequitable. The value of Plaintiff's and Class Members' behavioral data, when compiled, analyzed, and integrated into advertising algorithms or consumer profiling tools, constitutes a marketable asset in the digital economy. Defendant's ability to extract revenue from

this asset without disclosure or fair exchange renders its conduct unjust.

198. Under principles of equity and good conscience, Defendant should be required to disgorge all ill-gotten gains and benefits received as a result of its unjust enrichment at Plaintiff's and Class Members' expense.

XIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following:

1. An order certifying the Class, naming Plaintiff as Class representative, and naming Plaintiff's attorneys as Class counsel;
2. An order declaring that Defendant's conduct violates CIPA, the CCPA, the California Constitution, and Business & Professions Code § 17200;
3. An order declaring that Defendant's conduct unlawfully intrudes upon the seclusion of Plaintiff and the Class Members;
4. An order of judgment in favor of Plaintiff and the Class against Defendant on the causes of action asserted herein;
5. An order enjoining Defendant's conduct as alleged herein;
6. Disgorgement of profits resulting from unjust enrichment;
7. Statutory penalties;
8. Prejudgment interest;
9. Reasonable attorney's fees and costs; and
10. All other relief that would be just and proper as a matter of law or equity.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims so permitted.

Dated: May 24, 2025

MANNING LAW, APC

By: /s/ *Michael J. Manning*
Michael J. Manning, Esq.
Attorneys for Plaintiff

EXHIBIT A

TikTok Analytics

analytics.tiktok.com

Linkedin Insight Tag

px.ads.linkedin.com

Twitter Analytics

analytics.twitter.com

Globalsite Analytics

globalsiteanalytics.com

Google Tag Manager

www.googletagmanager.com

Invoca

solutions.invocacdn.com

Impact

utt.impactcdn.com