

**IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

ADRIAN VAZQUEZ, ALEXANDER
FOLEY, AND NICHOLAS ROSS, ON
BEHALF OF THEMSELVES AND ALL
OTHERS SIMILARLY SITUATED,

Case No. _____

CLASS ACTION

Plaintiffs,

v.

JURY TRIAL DEMANDED

KALSHI INC. AND KALSHIEX LLC,

Defendants.

CLASS ACTION COMPLAINT

Plaintiffs Adrian Vazquez, Alexander Foley and Nicholas Ross, on behalf of themselves and all others similarly situated, bring this class action complaint (“Action”) against Defendants Kalshi Inc. and KalshiEX LLC (“Kalshi” or “the Company”). The allegations below are based on Plaintiffs’ personal knowledge as to Plaintiffs’ individual experiences, the investigation of counsel, and information and belief.

INTRODUCTION

1. Kalshi owns and operates www.kalshi.com (the “Website”), an online platform that allows users to trade on the outcome of future events. Kalshi also owns and operates a mobile app (the “App”) that mirrors the Website (together “Digital Platforms”).

2. This is a class action brought on behalf of all individuals who accessed and used the Digital Platforms and whose communications, personally identifiable information (“PII”), and online activity were intercepted, disclosed, or transmitted to third parties without their consent.

3. Kalshi’s Digital Platforms are built around “event contracts.” Event contracts are contracts whose value depends on the outcome of a specified real-world event. On Kalshi, event

contracts are generally structured as binary “Yes” or “No” positions tied to a particular question.¹ A user who purchases a “Yes” contract takes the position that the event will occur. A user who purchases a “No” contract takes the position that the event will not occur.

4. Kalshi offers event contracts through the Website² and its App that are tied to the outcome of real-world events. Some real-world events—such as “Love Island USA S8: Winning Couple”—may be seen as trivial.³ Other event contracts/bets involve arguably more serious and sensitive events such as, “Will US Supreme Court ban transgender girls and women from competing on female sports teams?” and “When will traffic at the Strait of Hormuz return to normal?”⁴ Thus, the contracts a user views, researches, or trades can reveal private information about the user’s interests, beliefs, concerns, and predictions about real-world events.

5. Kalshi event contracts have a binary payout structure. If the user’s position is correct, the contract pays \$1.00 per contract. If the user’s position is incorrect, the contract pays \$0.00. A user’s gain or loss therefore depends on the price paid for the contract, the number of contracts purchased, the outcome of the event, and any applicable fees.

6. For example, if a Kalshi user buys a “Yes” contract for \$0.65, the user pays \$0.65 for a contract that will be worth \$1.00 if the event occurs and \$0.00 if the event does not occur. If the event occurs, the user receives \$1.00 and realizes a gross gain of \$0.35 before fees. If the event does not occur, the user receives nothing and loses the \$0.65 paid for the contract, plus any applicable fees.

¹ <https://kalshi.com/faq> (last visited June 25, 2026)

² www.kalshi.com/browse (last visited June 25, 2026)

³ <https://kalshi.com/category/culture> (last visited June 25, 2026)

⁴ <https://kalshi.com/category/politics> (last visited June 25, 2026)

7. Because event contracts require users to select a position on real-world events, a user's Kalshi activity can reveal the events the user considered important, the outcomes the user predicted, the amount of money the user was willing to risk, the user's confidence in particular outcomes, and the user's financial gains or losses. When linked to a verified account, device identifiers, location data, financial information, or third-party tracking technologies, this activity can reveal sensitive information about a user's beliefs, interests, behavior, and financial decision-making.

8. To use Kalshi's Digital Platforms, consumers must provide several categories of PII, including, *inter alia*, identity, contact and financial data. When consumers provide this information to Kalshi and use its Digital Platforms to research, view, and trade event contracts, they reasonably expect that their confidential information and user activity will be protected and will not be disclosed to unknown third parties without their knowledge or consent.

9. Those expectations are especially reasonable because Kalshi's Digital Platforms involve wagering-like activity that many consumers would consider private. There is a recognized stigma associated with gambling and gambling-adjacent conduct, particularly for individuals who struggle with compulsive gambling or gambling addiction.⁵ Users therefore have a heightened privacy interest in keeping their Kalshi activity confidential.

10. Although the Company identifies that it collects certain categories of data in its Privacy Policy, it does not require that users' consent (or even view) Kalshi's Policy to access or use its Website or App. Instead, Kalshi merely "recommend[s] reviewing" its Privacy Policy, and

⁵ See *Perceived social stigmatisation of gambling disorders and coping with stigma* <https://pmc.ncbi.nlm.nih.gov/articles/PMC8899262/> (last visited June 25, 2026); see also *Gambling Disorder and Stigma: Opportunities for Treatment and Prevention*, <https://pmc.ncbi.nlm.nih.gov/articles/PMC9440767/> (last visited June 23, 2026)

five other legally dense documents, but still allows new users to create an account without reading or affirmatively agreeing to any of the terms.

11. A person's trading and wagering-related activity is not ordinary browsing history. It can reveal what events the person follows, what outcomes the person predicts, how much money the person is willing to risk, how frequently the person returns to trade, and whether the person's activity reflects repeated or escalating engagement. When that activity concerns politics, elections, social controversies, sports, financial markets, armed conflict, or other real-world events, it can expose deeply personal information about the user's beliefs, interests, concerns, financial circumstances, and tolerance for risk.

12. Despite the sensitive nature of the information collected through its Digital Platforms, Kalshi installed and permitted third-party scripts, pixels, and tracking technologies to operate on the platforms. These technologies are lines of code or embedded tools supplied by outside vendors that allow those vendors to collect, receive, transmit, and analyze information about users and their interactions with a platform.

13. Through these tracking technologies, third parties such as Google, TikTok, LinkedIn, and others were able to monitor users as they interacted with Kalshi's Digital Platforms. This monitoring included, upon information and belief, users' browsing activity, pages viewed, event contracts reviewed, account interactions, and trades or attempted trades.

14. By embedding these trackers on its Digital Platforms, Kalshi aided third-party advertisers to collect, intercept, and transmit sensitive and confidential information submitted by Plaintiffs and members of the putative class, including activity that revealed what those event contracts users researched and trades they placed.

15. Kalshi knew or should have known that embedding third-party trackers on the Digital Platforms would lead to the interception, disclosure, and weaponization of user PII for advertising, analytics, profiling, and other commercial purposes.

16. Upon information and belief, Kalshi utilized data from trackers to improve its advertising and marketing campaigns, reduce customer-acquisition costs, increase trading activity, generate revenue, and to receive cash payments from the third parties receiving the data.

17. Plaintiffs and Class Members did not consent to Kalshi's disclosure of their PII and sensitive information about their beliefs, interests, behavior, and financial decision-making to third parties, for advertising purposes or otherwise.

18. To rectify Kalshi's misconduct, Plaintiffs, on behalf of themselves and all others similarly situated, bring this Action, seeking actual, punitive, and statutory damages, restitution, injunctive relief and a declaratory judgment, as well as pre- and post-judgment interest and reasonable costs and attorneys' fees.

JURISDICTION AND VENUE

19. **Subject Matter Jurisdiction.** This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000 exclusive of interests and costs, there are well over 100 putative Class members, and minimal diversity exists because one or more putative Class members are citizens of a different state than the Defendants. Plaintiffs Adrian Vazquez and Alexander Foley are citizens of Florida, Nicholas Ross is a citizen of Pennsylvania, and Kalshi is a Delaware corporation with its principal place of business in New York, New York.

20. **Personal Jurisdiction.** This Court has personal jurisdiction over Kalshi. because it is a resident of, and maintains its headquarters within, this District.

21. **Venue.** Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Kalshi conducts business in this District and a substantial part of the events, acts and omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

Plaintiffs

22. Plaintiff Adrian Vazquez ("Vazquez") is a citizen of the State of Florida residing in Hudson, FL. Plaintiff Vazquez used Kalshi's App to place numerous trades on multiple dates in June 2026

23. Plaintiff Alexander Foley ("Foley") is a citizen of the State of Florida residing in Lake Wales, FL. Plaintiff Foley created his account on the Website and used Kalshi's App to place numerous trades on multiple dates in June 2026.

24. Plaintiff Nicholas Ross ("Ross") is a citizen of the State of Pennsylvania residing in Pittsburgh, PA. Plaintiff Ross used Kalshi's Website and the App to place numerous trades on multiple dates in 2025 and 2026.

Defendants

25. Defendant Kalshi Inc. is a Delaware corporation with its principal place of business in New York, New York. Defendants develop, own, and operate the Digital Platforms, which are available throughout the United States.

26. Defendant KalshiEX LLC is a financial services company with its principal place of business in New York, New York. KalshiEX LLC is the wholly owned, federally regulated subsidiary that operates the Kalshi event-contract exchange.

FACTUAL ALLEGATIONS

A. Kalshi Tracks Habits of Its Users that are Sensitive and Should be Kept Private

27. The information that Kalshi collects from its users is sensitive, personally identifiable, and private. It is not limited to ordinary contact information. Kalshi collects and maintains data that links a user's real-world identity to the user's financial information, account activity, trading history, and activity on Kalshi's Digital Platforms.

28. To create and use a Kalshi account, users must provide PII, including sensitive information such as personal identity, contact, and financial information. Upon information and belief, Kalshi also collects and/ or maintains profile data, usage data, location data, device identifiers, IP addresses, cookies, unique account identifiers, trades, orders, interests, preferences, account balances, transaction history, and other information reflecting how users interact with the Digital Platforms.

29. Because Kalshi requires users to verify their personal identities, provide financial information, fund their accounts, and conduct trades through those accounts, users reasonably expect their identifiable account and trading activity to remain confidential. Kalshi operates a federally regulated contract market, maintains account balances and transaction histories, and processes trades through funded accounts. These features signal that Kalshi is handling sensitive financial and transactional information, and not merely anonymous browsing data, regardless of whether its products are characterized as event contracts, securities, or wagers.

30. The sensitive information at issue does not solely constitute who the user is, but also what the user does on Kalshi's Digital Platforms. A user's Kalshi activity can reveal the event contracts the user searched for, viewed, researched, followed, purchased, sold, or attempted to trade; whether the user took a "Yes" or "No" position; the price the user paid; the amount of money

the user risked; the user's open positions; the user's gains or losses; and the timing, frequency, and pattern of the user's activity.

31. This information is highly revealing because Kalshi event contracts are tied to real-world events. A user's activity on the Digital Platforms can therefore disclose the user's interests, beliefs, predictions, financial concerns, political views, social views, sports interests, geopolitical concerns, economic outlook, and tolerance for financial risk.

32. Users also reasonably expect privacy in information concerning their personal interests and behavior, particularly where that information concerns gambling or wagering-related activity. Federal regulators have recognized that companies increasingly collect and infer detailed information about consumers' interests and conduct in ways that exceed ordinary users' expectations. In a recent report, the FTC "found that the companies are gathering detailed personal information, such as the websites you visit, your location data, your demographic information, and your interests including sensitive interests."⁶

33. Regarding user interests, the FTC noted:

Of particular interest, some Companies revealed user interest categories that are more akin to Demographic Information. For example, some Companies' user interest categories revealed parental status (e.g., user interest category for "baby, kids and maternity") or marital status (e.g., "newlyweds" or "divorce support"). ***While such user interests may, at first glance, seem innocuous, the particularity of user interest categories often would have allowed the Company to infer more (and sometimes much more) information about a consumer.***⁷

⁶ *FTC Report Confirms: Commercial Surveillance is Out of Control* (Sept. 26, 2024), <https://www.eff.org/deeplinks/2024/09/ftc-report-confirms-commercial-surveillance-out-control> (last visited June 26, 2026) (emphasis added).

⁷ *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services* (September 11, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf (last visited June 26, 2026)

34. This practice identified by the FTC is often referred to as “behavioral advertising” and allows online actors to track, profile, and target particular people or types of people.⁸ The profiling aspect of behavioral advertising is particularly problematic as “[m]any targeting systems start with users’ behavior-based profiles, and then perform algorithmic audience selection, meaning advertisers don’t need to specify who they intend to reach.”⁹

35. This practice can often lead to predatory and/or discriminatory effects because advertisers can “use behavior-based profiles to target people based on *proxies* for such demographic characteristics, including ‘interests,’ location, purchase history, credit status, and income.”¹⁰

36. In the context of online gambling, profiling a user based on their interest of betting on sporting events is especially harmful because “digital gambling marketing strategies focused on vulnerable populations, including young people and problem gamblers or at-risk gamblers.”¹¹ The mechanism is engagement-driven: features and marketing are psychologically designed to nudge users toward action, and the combination of gamification and personalized marketing hits vulnerable users harder, encouraging more frequent engagement and deeper gambling behavior.¹²

⁸ *Ban Online Behavioral Advertising* (March 21, 2022), <https://www.eff.org/deeplinks/2022/03/ban-online-behavioral-advertising> (last visited June 26, 2026).

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Gambling Marketing Strategies and the Internet: What Do We Know? A Systematic Review* (Feb. 25, 2021)

<https://www.frontiersin.org/journals/psychiatry/articles/10.3389/fpsy.2021.583817/full> (last visited June 26, 2026)

¹² *Id.*

37. Indeed, “[m]any of these marketing tactics are designed to keep users engaged, spending, and chasing losses. What appears to be entertainment on the surface is actually a carefully engineered system meant to capture your attention and encourage impulsive behavior.”¹³

38. This phenomenon is not accidental. Rather, betting and wagering website operators, like Kalshi, combine data to build comprehensive behavioral profiles—such as frequency of visits, markets viewed, losses, deposits, time spent, and prior engagement—then monetize it through micro-targeted advertising designed to exploit psychological vulnerabilities and nudge users toward repeated engagement, posing heightened risks to vulnerable populations including individuals with gambling addictions.¹⁴

39. Behavioral advertising generally works by tracking users’ online activity, assigning them to categories or audiences, and serving them ads based on what they have done, viewed, clicked, searched, purchased, or otherwise revealed through their online behavior. Advertisers and advertising platforms can also use similar profiles to identify “lookalike” audiences—users who resemble existing customers or high-value users—and target them with additional advertising.

40. Although an individual’s interest in betting on events may seem innocuous when viewed in isolation, the data collected through the Digital Platforms can be used to build a detailed profile of that user’s wager-making interests, financial behavior, and vulnerabilities. That profile can then be used to target the user with advertising, re-engagement campaigns, recommendations, or other marketing designed to increase the user’s use of Kalshi’s platform.

¹³*The Rapid Growth Of Mobile Gambling And Sports Betting*, <https://www.addictioncenter.com/behavioral-addictions/gambling-addiction/rise-of-gambling-apps/> (last visited June 26, 2026).

¹⁴*See The Privacy Parlay: How Data Mining and Targeted Ads Drive Gambling Addiction* (Nov. 21, 2025), <https://sjpl.maine.gov/2025/11/21/the-privacy-parlay-how-data-mining-and-targeted-ads-drive-gambling-addiction/> (last visited June 26, 2026).

41. As described below, Kalshi disclosed Plaintiffs’ and putative Class Members’ PII and sensitive activity on the Digital Platforms—including information capable of identifying users and revealing the event contracts they viewed, searched for, researched, or traded to third-parties for advertising and other commercial purposes—without obtaining specific authorization from Plaintiffs and putative Class Members.

B. Tracking Technology Background

42. Online social media platforms derive revenue almost exclusively from selling targeted advertising to both the users of its own platform, and to internet users generally, by integrating web beacons, such as pixels and web bugs, and cookies onto websites. Meta, for example, generates billions of dollars in revenue, the vast majority of which derives from selling advertising space. Meta can generate such revenue through its ability to precisely target individual consumers.

43. A website does more than display pages to the people who visit it. Its operator can add small pieces of computer code—known as pixels, tags, cookies, and software development kits (“SDKs”)—that cause each visitor’s own web browser to send a copy of what the visitor is doing to outside companies.¹⁵ Operators add this code to show visitors advertising, to measure that advertising, to assemble audiences of users, and to follow visitors with ads after they leave the site.¹⁶

¹⁵ See *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FED. TRADE COMM’N (Mar. 16, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>; see also *Meta Pixel*, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/> (last visited June 26, 2026) (describing the Meta Pixel as “a snippet of JavaScript code that allows you to track visitor activity”).

¹⁶ See *About dynamic remarketing*, GOOGLE ADS HELP, <https://support.google.com/google-ads/answer/3124536?hl=en> (last visited June 26, 2026) (remarketing “allows you to show ads to customers who have previously visited your website”); *Conversion Tracking*, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion->

44. Social media platforms use pixels and similar tracking software to build profiles on web users that include real names, locations, email addresses, telephone numbers, purchasing habits, and communications that the companies associate with unique personal identifiers like IP addresses, browser fingerprints, device IDs and cookie identifiers.

45. By associating or assigning these identifiers to a particular individual, companies can track a user's behavior across websites to build a more detailed consumer profile. For example, Meta assigns what it calls a Facebook user ID to each individual user of its platform.¹⁷ A user's Facebook ID is associated with their Facebook profile, which typically includes diverse demographic and personal information such as user's location, photos, interests, employment history, relationship status, and other details.¹⁸ Since a Facebook ID serves as a unique identifier for an individual's Facebook account, Facebook or any regular person could utilize a Facebook ID to locate, access, and view a user's corresponding Facebook page.

46. Every website, including Kalshi, is hosted by a computer "server" that holds the website's contents. Through the server, the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

47. 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:

tracking/ (last visited June 26, 2026) (tracked conversions used to measure ad effectiveness and to define custom audiences).

¹⁷ See *Graph API User*, META FOR DEVELOPERS, <https://developers.facebook.com/docs/graph-api/reference/user/> (last visited June 25, 2026).

¹⁸ See *id.*

HTTP Request: electronic communication sent *from* the user device's browser to the website's server. Some HTTP requests, for example, can specify the particular URL visited by the user.

HTTP Response: an electronic communication that is sent *to* the user 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.

Cookies: a small text file that can be used to store information on the user device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from user 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.

48. In addition to the communication itself, embedded cookies and other tracking tools may also capture personal identifiers like a user ID, browser fingerprints, device IDs, and IP addresses.

49. On dates unknown and continuing to the present, Kalshi embedded tracking tools throughout its platform, allowing third parties to intercept the confidential interactions and communications of Plaintiffs and Class Members with the Website.

50. Upon information and belief, third parties also received the following information related to Plaintiffs and Class Members' interactions with Kalshi's Website: (1) the URL of specific pages browsed; (2) the time spent on each page; (3) the path taken to get to that page; and (4) certain actions, such as button clicks.

51. Kalshi intentionally configured the trackers installed on its Website to capture both the "characteristics" of individual users' communications with Kalshi's Website (their IP

addresses, account IDs, cookie identifiers, device identifiers and account numbers) and the “content” of these communications (the buttons, links, pages and tabs they click and view).

C. Kalshi’s Business and Tracking on Its Website

52. Kalshi owns and operates the Website, where users are invited to make trades across a wide variety of markets, including elections, politics, sports, culture, crypto, commodities, climate, economics, mentions, finance, and “tech & science.”¹⁹

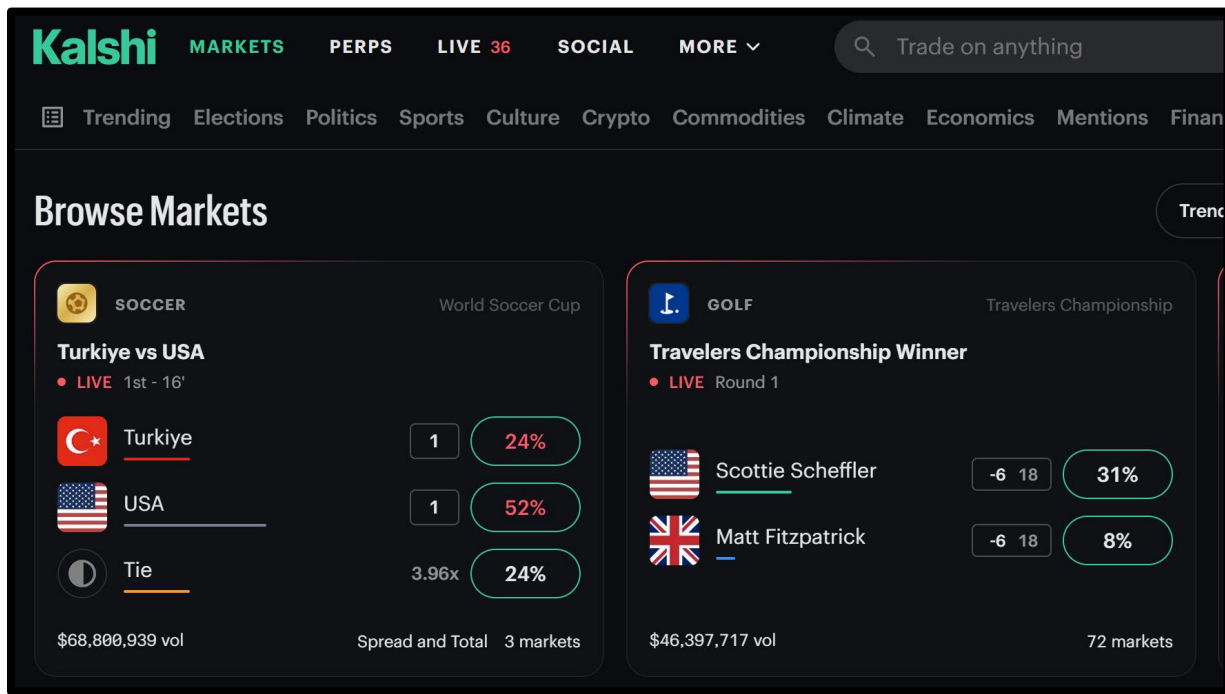


Figure 1. Kalshi Browser Page

53. When a user signs up for Kalshi, the user must verify an email address or sign in through a Google or Apple account. But account creation alone does not allow a user to trade. To make a trade the user must complete a digital identity-verification process.²⁰

54. During the digital verification process, users provide the following pieces of information: (1) full name, (2) date of birth, (3) phone number, (4) address and (5) any other

¹⁹ www.kalshi.com (last visited June 25, 2026)

²⁰ <https://kalshi.com/market-integrity/customer-identification> (last visited June 25, 2026)

information requested by Kalshi's third party identity verification vendor including, for example, a passport or driver's license or social security number.²¹

55. Once verified, a user has several options for how to fund their Kalshi account. Kalshi provides multiple funding methods – a user can link a debit card, bank account or crypto wallet, or deposit funds via card, bank, crypto, wire transfer, cash app, real-time payments, PayPal, and Venmo. Each of these funding options require a user to provide sensitive financial information to Kalshi.²²

56. After funding an account, a user may place a trade by selecting a market, choosing whether to buy or sell, selecting the “Yes” or “No” side of the contract, choosing a contract quantity or dollar amount, reviewing the order, and submitting the trade. That order flow reveals not merely that the user visited Kalshi, but the specific market the user selected, the outcome the user predicted, the amount of money the user was willing to risk, and the timing and frequency of the user's trading activity.

57. Kalshi begins tracking users from the moment they land on the Website via third party trackers. The trackers are configured to capture user interactions as they browse the Website, search for markets, view event contracts, click buttons, navigate between pages, create an account, verify their identity, fund the account, and ultimately place trades.

58. Kalshi places—or knowingly permits to be placed—multiple layers of third-party code on its Website that extracts the text that users input on the site (which can include a user's full name, date of birth, postal and email address, telephone number and financial information)

²¹ *Id.*

²² <https://help.kalshi.com/en/collections/18616608-deposits-withdrawals> (last visited June 25, 2026)

and data that reveals what those users are doing on the site (e.g., searches for trades and the placement of bets).

59. The resulting packets combine such sensitive information with unique digital identifiers and relay it to outside advertising, analytics, and content-recommendation companies.

60. Kalshi employs over 60 different third-party trackers on its website—some belonging to well-known ad-tech companies like Google and Meta and others to more obscure entities like HypeLab and Rokt—primarily for advertising and analytics purposes. These trackers run are placed throughout the Website, capturing various aspects of the user experience.

61. Kalshi users' most sensitive interaction with the Website—their placing of a bet—is captured by four trackers. These trackers fall into three categories:

- **Product-analytics SDK (Amplitude):** Amplitude is an AI analytics platform. Kalshi's placement of the SDK allows Amplitude to receive the following information: (1) which market you bet on; (2) that you placed a bet; (3) the dollar amount and order ID; (3) whether you bought or sold and bet "Yes" or "No"; (4) the steps you took; (5) pages you viewed and came from; (6) user ID and device ID; (7) operating system, language and browser; and (8) your approximate location.
- **Insight Tag Script (LinkedIn):** The LinkedIn Insight Tag is a third-party script that is often used to track users' online behavior. Kalshi's communication with the tracker allows LinkedIn to receive the following information: (1) which market you bet on; (2) that you placed a bet; (3) whether you bought or sold and bet "Yes" or No (via URL parameters); (4) buttons pressed; (5) URL and page title; (6) partner ID; (7) operating system and browser; and (8) your approximate location.

- **Advertising and Attribution Pixels (TikTok and AppLovin):** The

TikTok Pixel and AppLovin Pixel are third-party advertising pixels.

- The TikTok Pixel: The TikTok pixel is deployed via a Google Tag Manager that is used to manage analytics and marketing code. Kalshi's inclusion of this tracker allows TikTok to receive the following information: (1) which market you bet on; (2) that you placed a bet; (3) whether you bought or sold and bet "Yes" or No (via URL parameters); (4) buttons pressed; (5) URL and referrer page; (6) session count (7) unique user ID; (8) operating system and browser; and (9) your approximate location

- The AppLovin Pixel: AppLovin is mobile ad company that helps consumer brands and gaming apps scale their business profitably. The AppLovin pixel is deployed using a tracker called Axon. Kalshi's inclusion of the AppLovin pixel allows AppLovin to receive the following information: (1) which market you bet on; (2) that you placed a bet; (3) currency used; (4) whether you bought or sold and bet "Yes" or No (via URL parameters); (5) buttons pressed; (6) URL and referrer page; (7) the number of the current visit and the dates and times of all previous visits; (8) unique user ID; (9) operating screen and window size; and (10) your approximate location

62. The mentioned scripts fire on the pages that expose the very placement of a bet that users expect to remain private—including identifying information, what markets one is betting, whether one bet "Yes" or "No", the number of visits and other personal information.

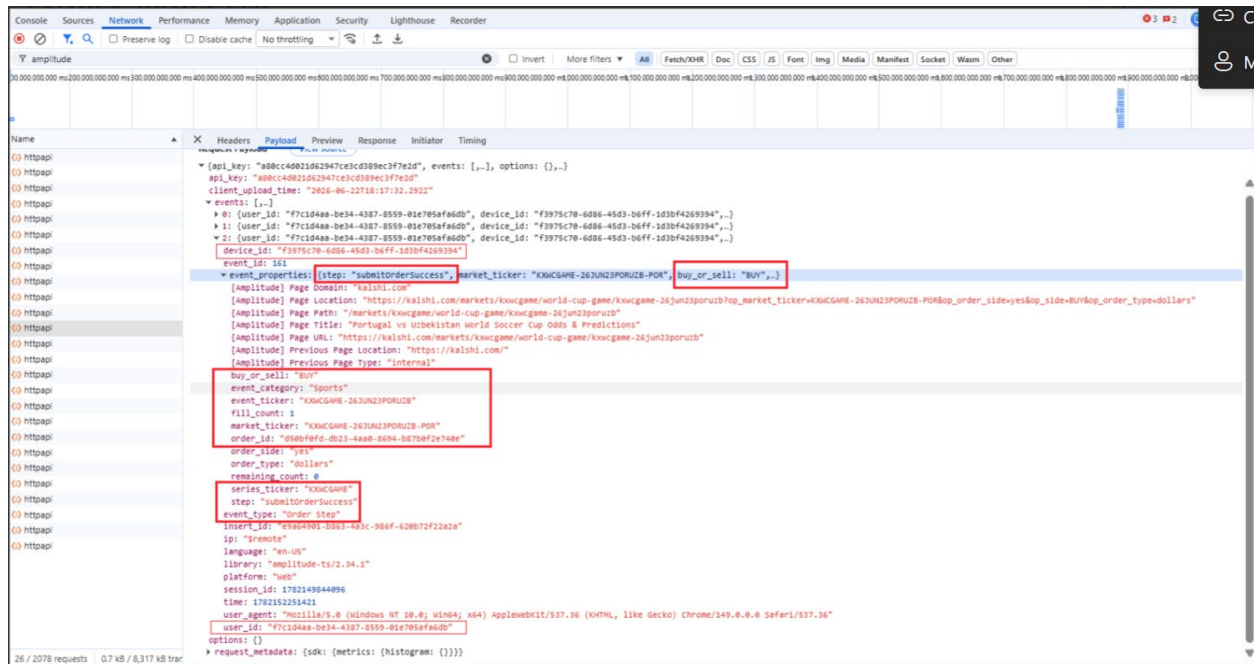


Figure 2. Trade Related Data Sent to Amplitude

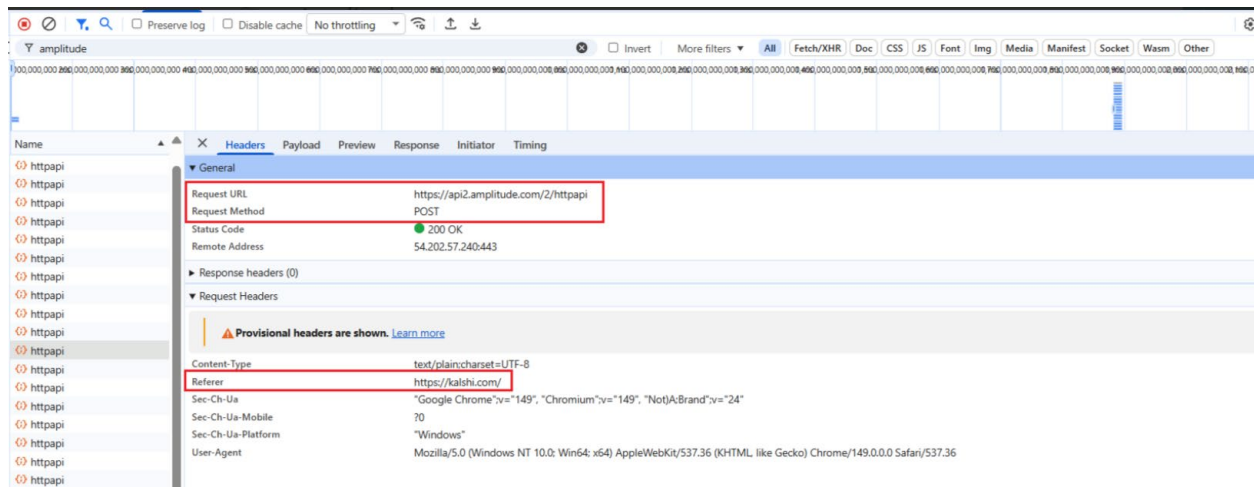


Figure 3. Request for Data from Amplitude

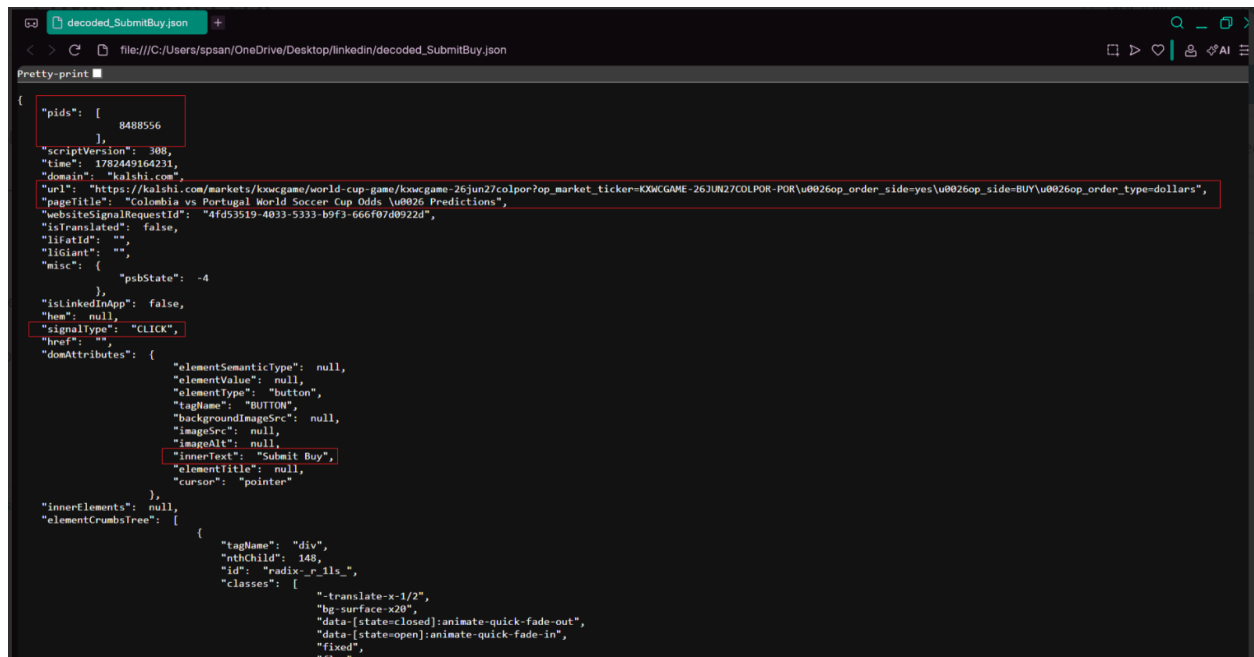


Figure 4. Trade Related Data Sent to LinkedIn

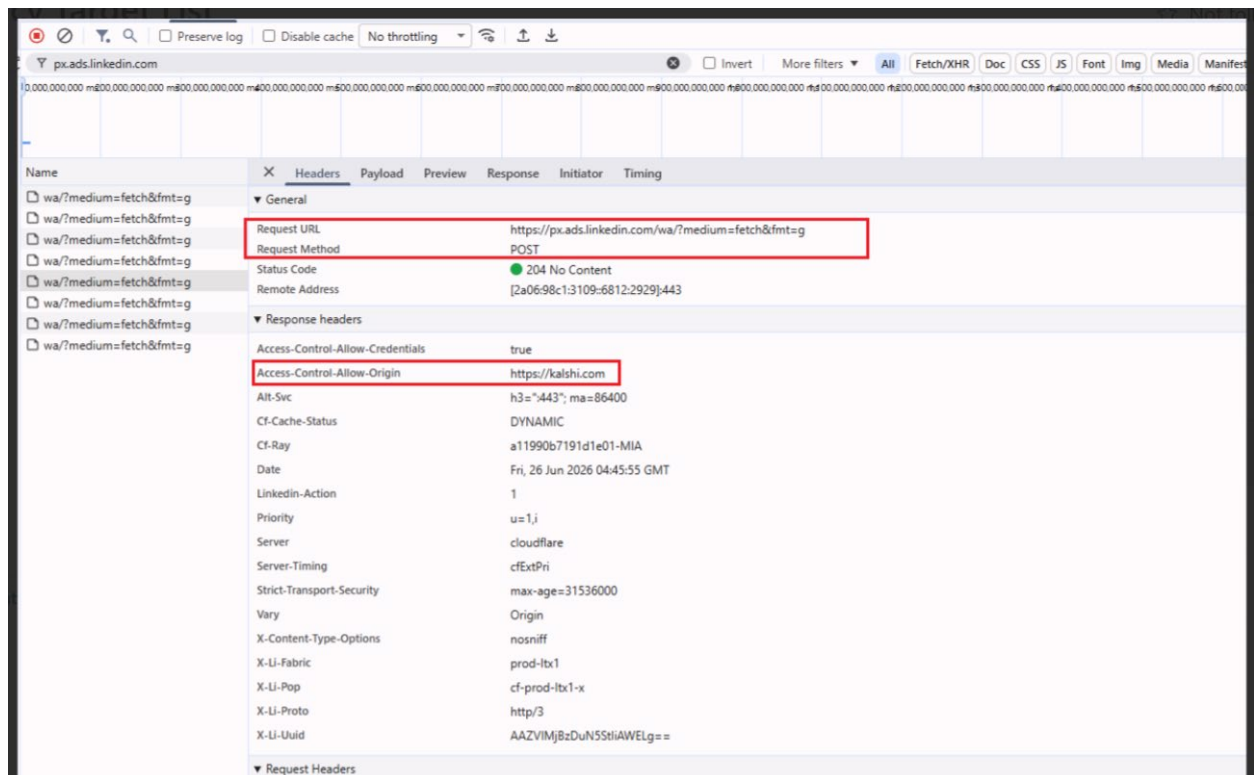


Figure 5. Request for Data from LinkedIn

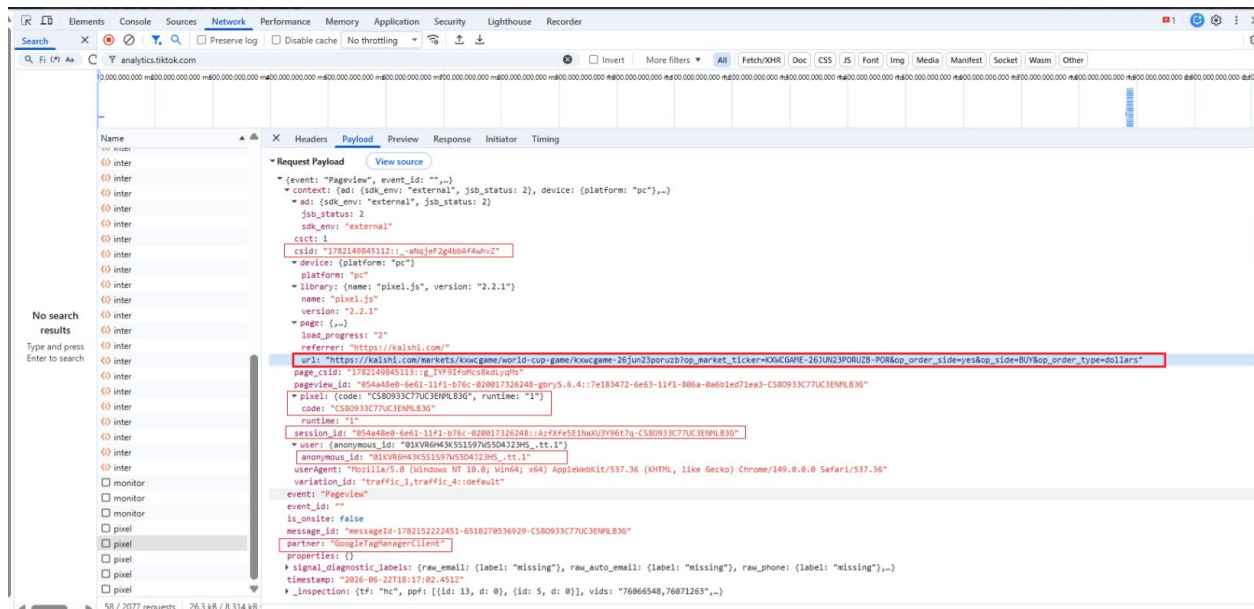


Figure 6. Trade Related Data Sent to TikTok

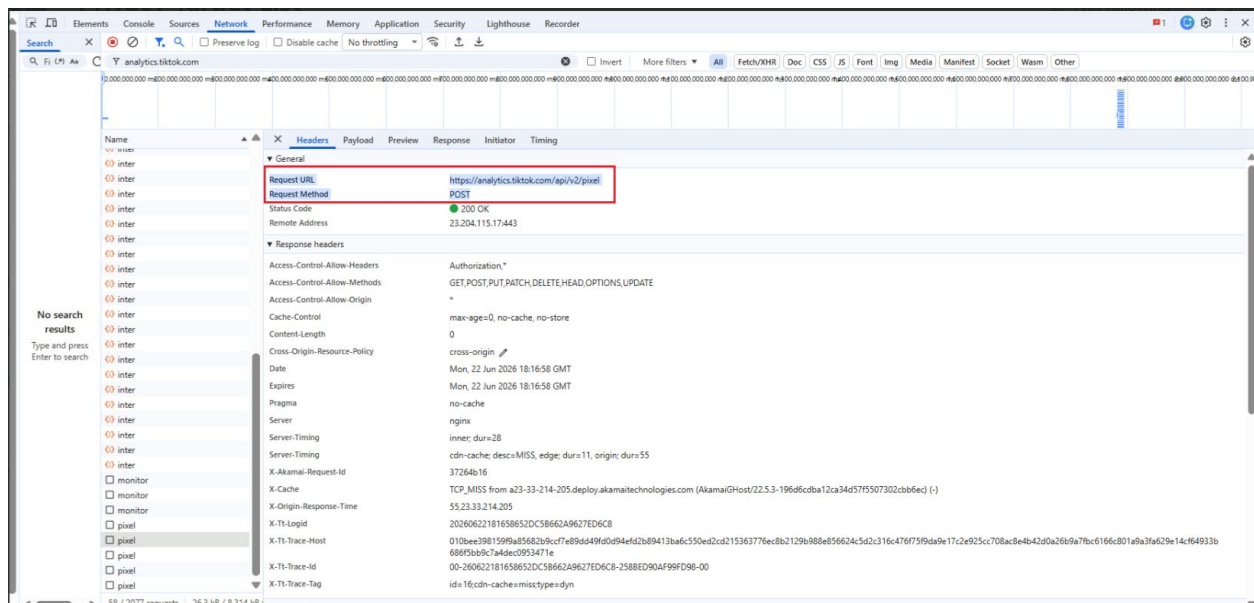


Figure 7. Request for Data from TikTok

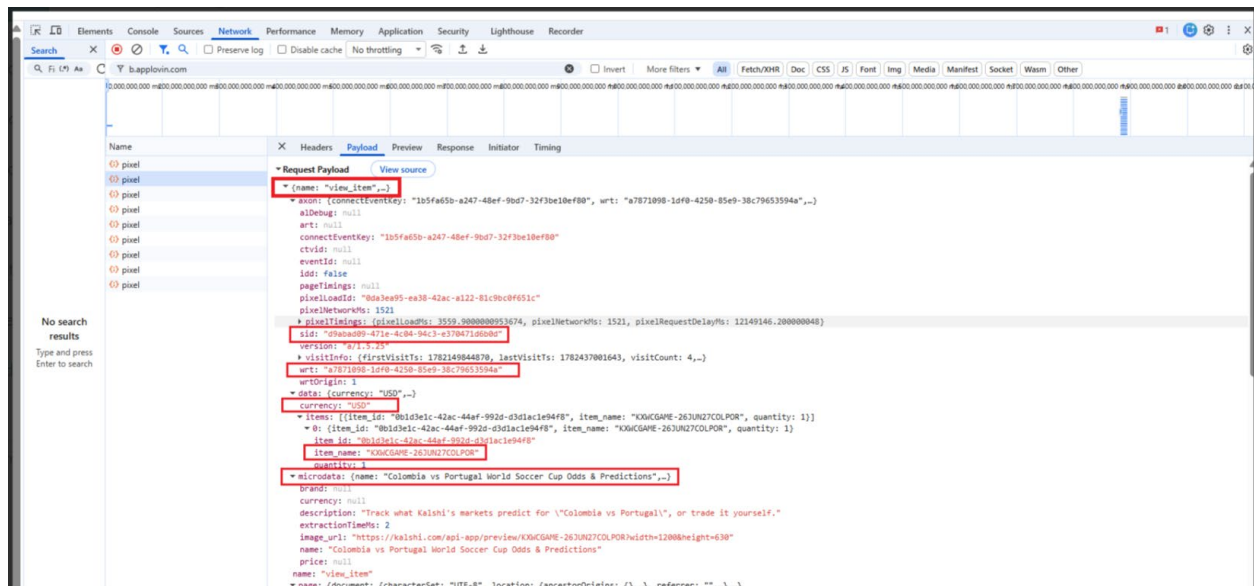


Figure 8. Trade Related Data Sent to AppLovin

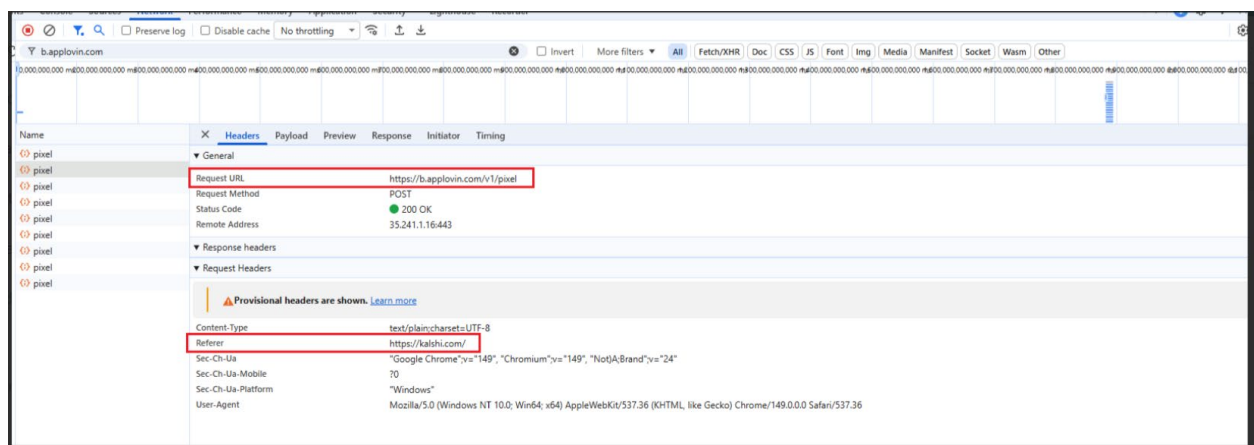


Figure 9. Request for Data from AppLovin

63. Through this architecture, Kalshi knowingly lets third parties collect, and monetize information that reveals a user's PII as well as their wagering patterns and preferences.

64. Disturbingly, Kalshi also keeps track of the number of visits that a user has made to the Website as well as the dates and times of all previous visits. This information in combination with information regarding which markets were wagered is exactly the kind of user interest data that is of great help to Kalshi, but great harm to its users.

65. Kalshi's covert data-sharing scheme is not a mistake, but rather a deliberate business practice where Kalshi trades the privacy of its user for advertising reach and profit.

C. Kalshi's Failed to Obtain Users' Consent

66. Kalshi fails to give users a clear and conspicuous opportunity to refuse or withdraw consent to any of the interceptions and sharing on a case-by-case basis.

67. At no point does Kalshi plainly inform visitors of its Website that their interaction may be intercepted and shared with third parties. Nor does the Website provide a straightforward mechanism to decline or revoke that sharing.

68. Kalshi's home screen, which a user would see upon entering the Website, looks as follows:

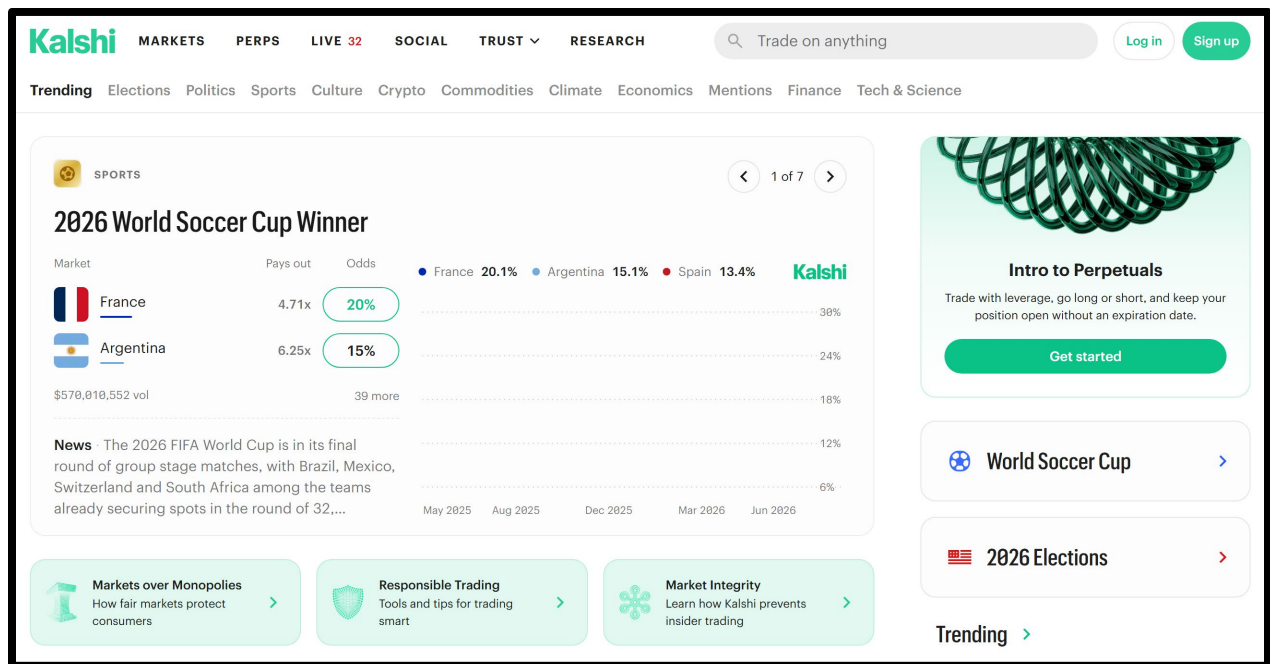


Figure 10.

69. To create an account, a user must go to the top right and click "Sign up." Upon clicking, "Sign up," the user is presented with the following sign up banner:

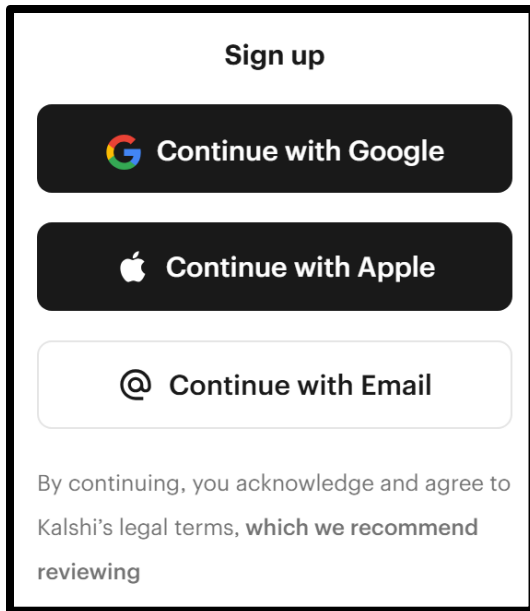


Figure 11.

70. As Figure 11 shows, a user is never required to take any affirmative step to agree to Kalshi's legal terms or to confirm that they have reviewed them. The banner states only that, “[b]y continuing, you acknowledge and agree to Kalshi’s legal terms, which we recommend reviewing.” Although the phrase “legal terms” hyperlinks to the documents Kalshi claims to recommend reviewing, it bears none of the customary indicia of a hyperlink: it is not rendered in a contrasting color, it is not underlined, and it is otherwise indistinguishable from the surrounding white text.

71. If a user happens to come across the hyperlink and clicks it, they are met with a list of six legal documents, as shown in Figure 12 below. A user is not required to review or scroll through any of these documents before creating an account.

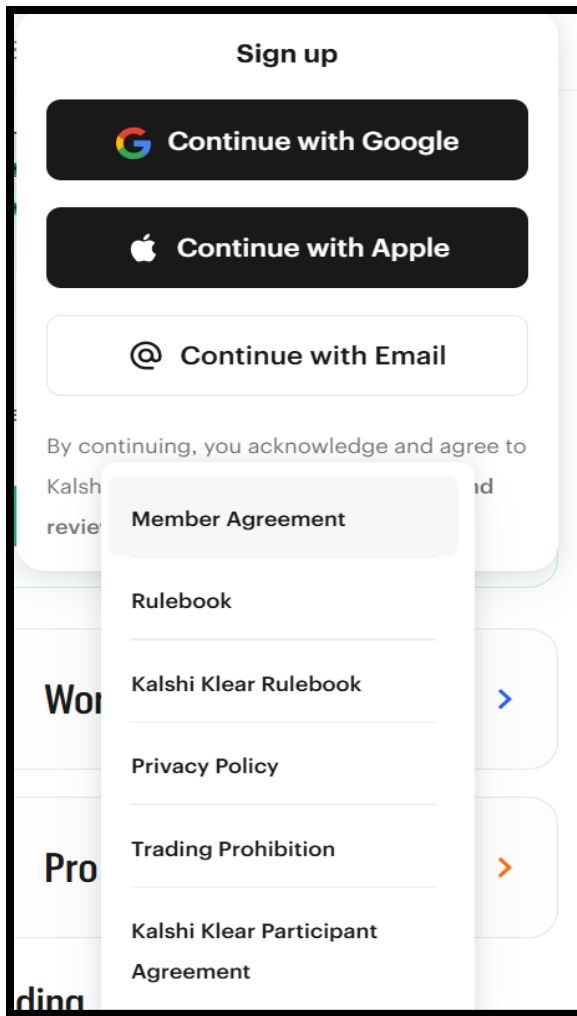


Figure 12.

72. The sign up banner is found at the top right corner of the Website. As shown in Figure 13 below, the user's attention is dominated by a dense array of trading information—market listings, live odds, price charts, trending events, and navigation across more than a dozen categories—that crowds the screen and draws the eye away from the nearly invisible privacy-disclosure hyperlink tucked within the sign up panel.

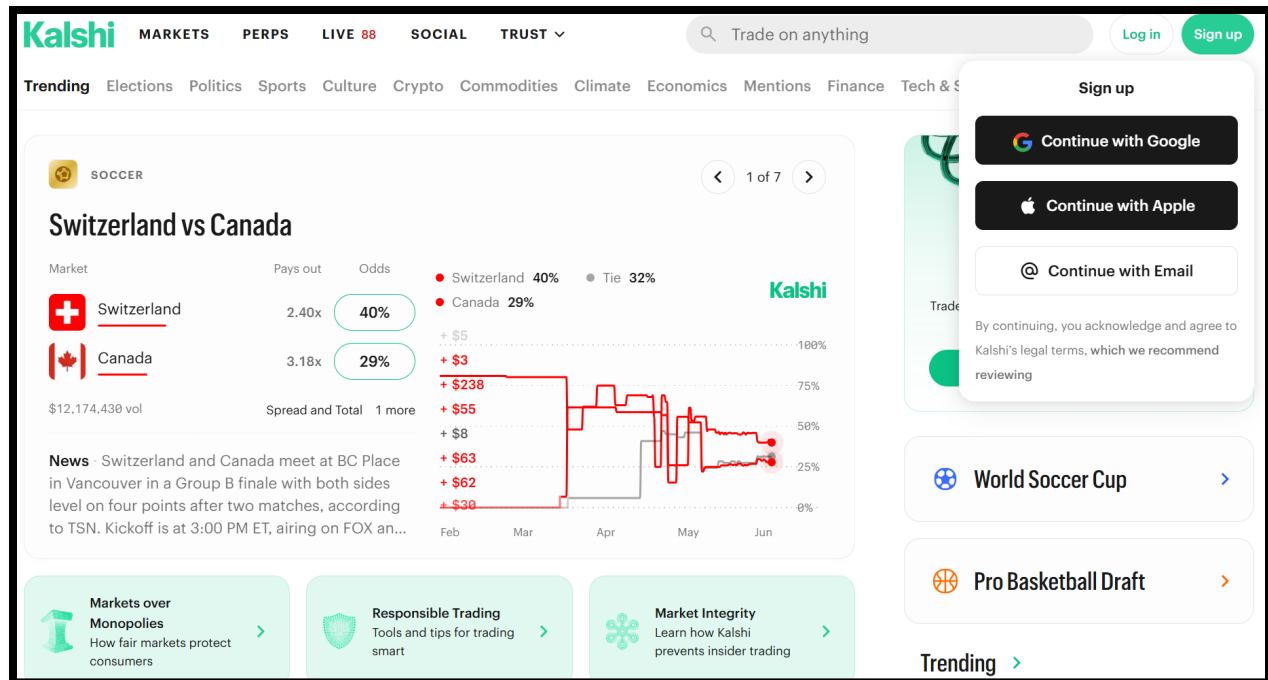


Figure 13.

73. As mentioned, Kalshi further deemphasizes the hyperlink by failing to use common design cues—such as underlining or distinct coloration like blue or red to indicate that the text is clickable.

74. Kalshi’s design choices fall short of giving users adequate notice or an opportunity to consent to its Privacy Policy.

75. In addition: “Kalshi is regulated by the Commodity Futures Trading Commission (CFTC). Kalshi is regulated as a Designated Contract Market (DCM), which is an exchange designated by the CFTC to trade swaps, futures and options under the Commodity Exchange Act.”²³

²³ <https://kalshi.com/about> (last accessed July 8, 2026).

76. As part of its regulatory obligations under the CFTC, Kalshi maintains and publicly files a Rulebook governing the operation of its exchange and Kalshi's treatment of information obtained from market participants.²⁴

77. Kalshi's Rulebook forms part of the rules governing Kalshi's federally regulated exchange and establishes restrictions on how Kalshi may use and disclose participant information.²⁵

78. Rule 11.1 of the Kalshi Rulebook expressly distinguishes "Personal Information" and "Proprietary Data" from ordinary public market information and imposes restrictions on Kalshi's use and disclosure of that information.²⁶

79. Rule 11.1(d) dictates that transaction data shall not be disclosed publicly "other than on an aggregated or anonymous basis, or in a manner that does not directly or indirectly identify any Participant who has submitted such data."²⁷

80. This provision reflects Kalshi's own recognition that identifiable transaction data is confidential and should not be treated like ordinary public market information. It also recognizes that data can identify a participant indirectly, including through identifiers that permit transaction activity to be linked to a particular account, user, browser, or device.²⁸

81. Rule 11.1(e) also provides: "Kalshi shall not condition access to the Company upon a Participant's consent to the use of Proprietary Data and Personal information for business

²⁴ KalshiEX LLC Rulebook (2025), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cftc.gov/sites/default/files/filings/orgrules/25/07/rules07012525155.pdf (last visited July 8, 2026).

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

²⁸ *Id.*

or marketing purposes. Proprietary Data and Personal Information may not be used by the Company for business and marketing purposes *unless the Participant has clearly consented* to the use of Proprietary Data and Personal Information in such manner.”²⁹

82. Kalshi’s Rulebook therefore distinguishes between consent necessary to access and use the exchange and consent to use participant information for business or marketing purposes. Under Kalshi’s own rules, access to the exchange may not be conditioned on a participant surrendering control over the marketing use of personal or proprietary information.

83. Nevertheless, Kalshi did not present Plaintiffs and Class Members with a separate, optional, and clearly described choice concerning the use of their Personal Information, Proprietary Data, or transaction-related activity for advertising or marketing purposes.

84. Instead, Kalshi required users to proceed through a bundled sign-up process and purported to obtain assent to multiple legal documents as a condition of creating an account and trading on the exchange. Users could not decline the provisions concerning data use while retaining access to Kalshi’s trading services.

85. Mandatory acceptance of bundled account terms does not constitute the separate and clear consent contemplated by Kalshi’s Rulebook, particularly where users were not plainly informed that their identifiable market views, order-flow activity, “Yes” or “No” selections, buy or sell decisions, dollar amounts, and completed trades would be transmitted to third-party advertising, social-media, attribution, or analytics companies.

86. Nor did Kalshi provide just-in-time notice at the moment users viewed markets, selected positions, entered orders, or placed trades. Kalshi did not inform users that, contemporaneously with those actions, embedded tracking technologies would cause their

²⁹ *Id.* (emphasis added).

browsers or devices to transmit trade-related communications and persistent identifiers to outside companies.

87. Kalshi's own Rulebook therefore confirms that Plaintiffs and Class Members reasonably expected their identifiable transaction information, Personal Information, and Proprietary Data to remain confidential unless they separately and clearly consented to its use for business or marketing purposes.

88. The Rulebook also demonstrates that Kalshi knew the difference between disclosures necessary to operate and regulate its exchange and disclosures made for advertising or marketing purposes and knew that the latter required clear consent.

89. Notwithstanding those requirements and expectations, Kalshi caused or permitted Plaintiffs' and Class Members' identifiable market and trading activity to be transmitted to third-party advertising, analytics, attribution, and social-media companies without obtaining prior, clear, specific, and voluntary consent.

D. Kalshi's App Is Also Tracking Its Users Habits and PII

90. Kalshi also owns and operates the App, which can be used to make trades in the same markets as are available on the Website.

91. Upon information and belief, Kalshi is tracking PII and user habits in the App in addition to tracking this information across its Website.

92. Given the convenience of placing trades on the App, Kalshi would, upon information and belief, be incentivized to place identical or substantially similar trackers on the App to capture the same PII and user activity that it does on the Website.

93. Kalshi, however, fails to give users a clear and conspicuous opportunity to refuse or withdraw consent to any of the interceptions and sharing on a case-by-case basis.

94. As with the Website, at no point does Kalshi plainly inform visitors of its App that their interaction may be intercepted and shared with third parties. Nor does the App provide a straightforward mechanism to decline or revoke that sharing.

95. Kalshi's sign-up screen, which a user would see upon downloading the App, looks as follows:

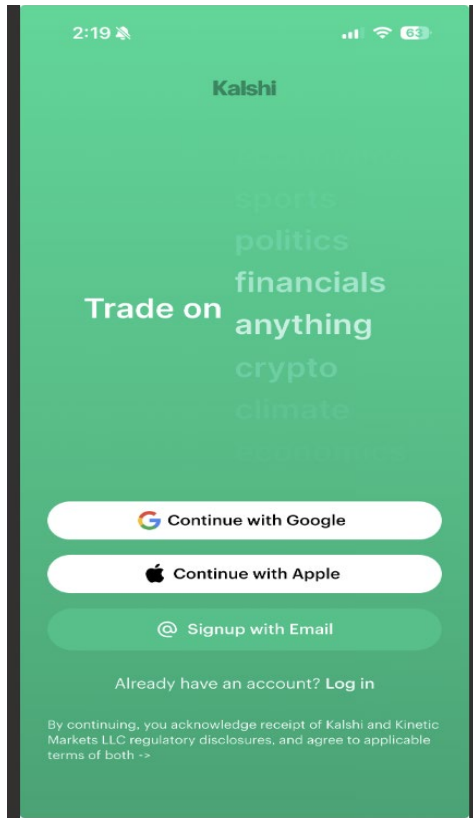


Figure 14.

96. As Figure 14 shows, a user is never required to take any affirmative step to agree to Kalshi's legal terms or to confirm that they have reviewed them. The banner states only that, "[b]y continuing, you acknowledge receipt of Kalshi and Kinetic Markets LLC regulatory disclosures and agree to applicable terms of both." Unlike the Website, the App fails to include a recommendation that these documents even be read. It is also an even less identifiable hyperlink

that that on the Website: there is one tiny arrow that will launch the disclosures, and it is not distinct from the language around it.

97. If a user happens to come across the hyperlink and clicks it, they are met with a list of eight legal documents, as shown in Figure 15 below. A user is not required to review or scroll through any of these documents before creating an account.

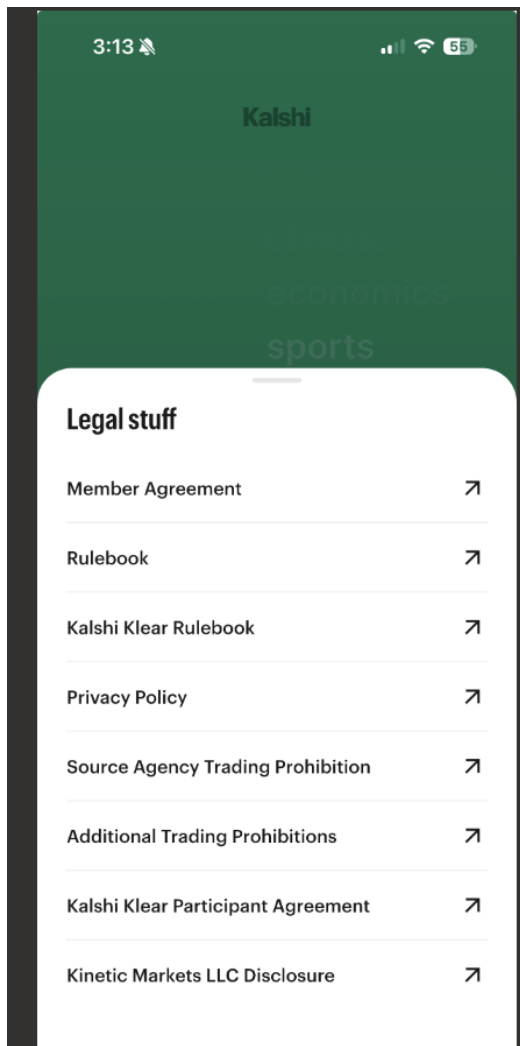


Figure 15.

98. As with its Website, Kalshi's design choices for the App fall short of giving users adequate notice or an opportunity to consent to its Privacy Policy.

E. Plaintiffs' Data Is Valuable

99. Plaintiffs' and Class Members' PII and Digital Platforms activity have value.

100. The data at issue here is valuable not only because it can identify Plaintiffs and Class Members, but because it links their identities and devices to sensitive behavioral and financial activity on Kalshi's Digital Platforms. This includes the markets users searched for or viewed, the event contracts they considered, whether they selected "Yes" or "No," whether they bought or sold, the amount of money they risked, the frequency and timing of their visits, their order-flow activity, and their trading patterns.

101. This information is valuable because it reflects real-time intent and highly specific consumer behavior. A user who repeatedly searches for or trades event contracts involving sports, elections, cryptocurrency, financial markets, or geopolitical events reveals actionable information about that user's interests, predictions, risk tolerance, and likelihood of returning to the Digital Platforms to place additional trades.

102. There is a significant market for data like that which Kalshi collected on the Digital Platforms and disclosed to third parties. Advertising and analytics companies use such data to identify users, track them across websites and devices, create behavioral profiles, build advertising audiences, measure conversions, attribute sales to advertisements, retarget users, and identify other users who resemble existing customers.

103. Kalshi's disclosure of Plaintiffs' and Class Members' data to third parties therefore deprived them of the economic value of the data itself. Plaintiffs and Class Members had the right to control whether, when, how, and to whom their PII and sensitive Digital Platforms activity would be disclosed. By disclosing that information to third parties without authorization, Kalshi

took for itself and its advertising partners a commercially valuable asset that belonged to Plaintiffs and Class Members.

104. Kalshi benefited from this unauthorized data disclosure. Upon information and belief, Kalshi used third-party trackers to improve marketing efficiency, attribute user activity to advertising campaigns, retarget users who visited or interacted with the Digital Platform, create advertising audiences, identify users likely to trade, reduce customer-acquisition costs, increase user engagement, and generate additional revenue from trading activity.

105. Kalshi's benefit did not depend on receiving a direct cash payment from each third party. The receipt of advertising, analytics, attribution, audience-building, conversion-measurement, and retargeting services constitutes valuable consideration. Those services are valuable precisely because they depend on the collection and use of Plaintiffs' and Class Members' PII and Digital Platform activity.

106. The value of such data as a commodity is measurable. As stated in "Exploring the Economics of Personal Data,"³⁰ "[f]irms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks." Consumer PII is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years. Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user from mining and selling data.³¹ That figure is due to keep increasing.

³⁰ *OECD Digital Economy Papers*, No. 220, OECD Publishing, Paris, <https://doi.org/10.1787/5k486qtxldmq-en>. (last visited June 26, 2026).

³¹ See Robert J. Shapiro, *What Your Data is Really Worth to Facebook*, Washington Monthly (July 12, 2019), <https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook> (last accessed June 26, 2026).

107. There is also a market for data in which consumers can participate. Courts have recognized PII has value. *See In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (“Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.”). Google has recognized the value of user data and even instituted a pilot program to pay users \$3 per week to allow Google to track them online.³²

108. The existence of consumer-facing data markets confirms that Plaintiffs’ and Class Members’ data has monetary value. Companies such as Nielsen, UpVoice, HoneyGain, and SavvyConnect pay for browsing historical information. Facebook also has paid users for their digital information, including browsing history. Until 2019, Facebook ran a “Facebook Research” app through which it paid \$20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35. These programs demonstrate that consumers can and do exchange access to their data for value when they are given notice and a meaningful choice.

109. Kalshi denied Plaintiffs and Class Members that choice. Plaintiffs and Class Members did not agree to license their PII, communications, trading activity, browsing history, or wagering-related behavioral data to third-party advertising and analytics companies. Nor did Kalshi compensate Plaintiffs and Class Members for the value it extracted from their data.

³² See Josh Sidorowicz, *Yes, Google will pay you to track what you do on your phone*, WTSP Tampa Bay 10 (Apr. 11, 2024), <https://www.wtsp.com/article/news/verify/google-tracking-study-payment-verify/67-1cc2e9a3-f51b-489b-ae8-1477201c0c11> (last accessed June 26, 2026).

110. The harm is especially acute because the data at issue concerns wagering-like conduct. Disclosure of a user's Kalshi activity can reveal not only that the user visited a prediction-market platform, but also the specific markets the user considered, the outcomes the user predicted, the amount of money the user was willing to risk, and the frequency with which the user returned to the Digital Platforms. This data can be used to identify vulnerable users, target repeat users, and encourage additional engagement with event-contract trading.

111. As a result of Kalshi's conduct, Plaintiffs and Class Members suffered economic injury, including loss of the value of their PII and sensitive Digital Platform activity, loss of control over the commercial use of their data, deprivation of the ability to decide whether to disclose or license that data, and the uncompensated taking of data that Kalshi and its third-party tracking partners used for commercial gain.

E. Plaintiffs' Experience with Kalshi

Representative Plaintiff Adrian Vazquez

112. Plaintiff Adrian Vazquez is and at all relevant times has been a resident of Hudson, Florida.

113. Plaintiff Vazquez has had an account with Kalshi since approximately June 2026, signing up with his real name and email address.

114. Because Plaintiff Vazquez's profile contains his legal name, Plaintiff Vazquez can be identified with that information.

115. On or around June 2026, Plaintiff Vazquez accessed the App and placed a trade with Kalshi.

116. As part of his use of the Digital Platforms, Plaintiff Vazquez visited multiple pages, including those for the trades he ended up placing.

117. During the process of that trade, Defendants disclosed his communications and PII to Amplitude, LinkedIn, TikTok, and AppLovin.

118. Each time Plaintiff Vazquez visited one of the Website pages, Defendants disclosed his event data, including the URL of pages visited, to Amplitude, LinkedIn, TikTok, and AppLovin.

119. Plaintiff Vazquez did not consent to the disclosure of his PII and Defendants did not attempt to obtain Plaintiff's consent before allowing Plaintiff to trade on the Website.

120. Plaintiff Vazquez was harmed by Defendants' data-sharing scheme and lost control over his personal information as a result.

Representative Plaintiff Alexander Foley

121. Plaintiff Alexander Foley is and at all relevant times has been a resident of Lake Wales, FL.

122. Plaintiff Foley has had an account with Kalshi since approximately June 2026, signing up with his real name and email address.

123. Because Plaintiff Foley's profile contains his legal name, Plaintiff Foley can be identified with that information.

124. On or around June 2026, Plaintiff Foley accessed the Digital Platforms and placed a trade with Kalshi.

125. As part of his use of the Digital Platforms, Plaintiff Foley visited multiple pages, including those for the trades he ended up placing.

126. During the process of that trade, Defendants disclosed his communications and PII to Amplitude, LinkedIn, TikTok, and AppLovin.

127. Each time Plaintiff Foley visited one of the Website pages, Defendants disclosed his event data, including the URL of pages visited, to Amplitude, LinkedIn, TikTok, and AppLovin.

128. Plaintiff Foley did not consent to the disclosure of his PII and Defendants did not attempt to obtain Plaintiff Foley's consent before allowing Plaintiff Foley to trade on the Website.

129. Plaintiff Foley was harmed by Defendants' data-sharing scheme and lost control over his personal information as a result.

Representative Nicholas Ross

130. Plaintiff Nicholas Ross is and at all relevant times has been a resident of Pittsburgh, PA.

131. Plaintiff Ross has had an account with Kalshi since approximately April 2025, signing up with his real name and email address.

132. Because Plaintiff Ross's profile contains his legal name, Plaintiff Ross can be identified with that information.

133. On or around April 2025 and at other times in 2025 and 2026, Plaintiff Ross accessed the Digital Platforms and placed a trade with Kalshi.

134. As part of his use of the Digital Platforms, Plaintiff Ross visited multiple pages, including those for the trades he ended up placing.

135. During the process of that trade, Defendants disclosed his communications and PII to Amplitude, LinkedIn, TikTok, and AppLovin.

136. Each time Plaintiff Ross visited one of the Website pages, Defendants disclosed his event data, including the URL of pages visited, to Amplitude, LinkedIn, TikTok, and AppLovin.

137. Plaintiff Ross did not consent to the disclosure of his PII and Defendants did not attempt to obtain Plaintiff's consent before allowing Plaintiff Ross to trade on the Website.

138. Plaintiff Ross was harmed by Defendants' data-sharing scheme and lost control over his personal information as a result.

TOLLING

139. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know (and had no way of knowing) that their PII was intercepted and unlawfully disclosed third parties because Defendants kept this information secret. Alternatively, applicable statutes of limitations have been tolled by other applicable rules or doctrines.

CLASS ACTION ALLEGATIONS

140. Plaintiffs bring this Action pursuant to Federal Rule of Civil Procedure 23, individually and on behalf of the following Class:

Nationwide Class: All natural persons in the United States who placed an event-contract trade on Kalshi's Digital Platforms and whose information about their betting, trading, or Digital Platform activity was collected and relayed to third parties by embedded tracking technologies.

141. In addition, Plaintiffs Adrian Vazquez and Alexander Foley plead the following subclass:

Florida Class: All natural persons in the State of Florida who placed an event-contract trade on Kalshi's Digital Platforms and whose information about their betting, trading, or Digital Platform activity was collected and relayed to third parties by embedded tracking technologies.

142. In addition, Plaintiff Nicholas Ross pleads the following subclass:

Pennsylvania Class: All natural persons in the State of Pennsylvania who placed an event-contract trade on Kalshi's Website and whose information about their betting, trading, and Website activity was collected and relayed to third parties by embedded tracking technologies.

143. The Nationwide Class Florida Subclass, and Pennsylvania Subclass are referred to in this Section together as the “Class.”

144. Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and any members of their immediate families; (2) the Defendants, Defendants’ subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendants or its parents have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiffs’ counsel and Defendants’ counsel.

145. **Numerosity.** The exact number of members of the Class is unknown and unavailable to Plaintiffs at this time, but individual joinder in this case is impracticable. The Class likely consists of hundreds of thousands of individuals, and the members can be identified through Defendants’ records.

146. **Typicality.** Plaintiffs’ claims are typical of the claims of the other members of the Class and arise from the same conduct by Defendants and are based on the same legal theories.

147. **Adequate Representation.** Plaintiffs have and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiffs have retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiffs have no interest that is antagonistic to the interests of the Class, and Defendants has no defenses unique to the Plaintiffs. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to the interests of the other members of the Class.

148. **Commonality and Predominance.** The Class’s claims present common questions of law and fact, and those questions predominate over any questions that may affect individual

Class members. Common questions for the Class include, but are not limited to, the following: whether Kalshi embedded tracking technologies on the Digital Platforms that disclosed Class members' communications and personal information to third parties; whether Defendants' conduct violated the Florida Security of Communications Act; whether Defendants' conduct violated the Pennsylvania Wiretapping and Electronic Surveillance Control Act and the appropriate scope and form of declaratory, injunctive, and monetary relief.

149. **Superiority.** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

150. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CAUSES OF ACTION

COUNT I

VIOLATIONS OF THE FLORIDA SECURITY OF COMMUNICATIONS ACT, FLA. STAT. §§ 934.01 et seq. (On behalf of the Florida Subclass)

151. Plaintiffs Adrian Vazquez and Alexander Foley re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein, and brings this Count individually and on behalf of the Florida Subclass against Defendants.

152. The Florida Security of Communications Act (“FSCA”) prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept any wire, oral, or electronic communication without the prior consent of all parties to the communication. Fla. Stat. § 934.03(1)(a)–(c). The FSCA further prohibits the use or disclosure of the contents of intercepted communications. Fla. Stat. § 934.03(1)(d)–(e).

153. Plaintiffs Adrian Vazquez and Alexander Foley’s and Florida Subclass members’ interactions with the Digital Platforms are “electronic communications” under the FSCA. These communications included, among other things, the transfer of data, signals, writings, requests, responses, form-field entries they submitted while creating their accounts, searches, clicks, page views, account interactions, order-flow activity, and event-contract trade information between users’ browsers or devices and Kalshi’s Digital Platforms.

154. Kalshi intentionally embedded and operated various third-party trackers on its Digital Platforms. These trackers were designed and configured to duplicate, record, and transmit the contents of users’ interactions—including page views, button clicks, form-field entries, and other behavioral metadata—to third-party servers in real time, contemporaneously with the user’s communication with Kalshi.

155. The information intercepted and disclosed by Kalshi and its third-party tracking partners included the “contents” of Plaintiffs Adrian Vazquez and Alexander Foley’s and Florida Subclass members’ electronic communications because it revealed the substance, purport, and meaning of their communications with Kalshi. This information included, upon information and belief, the Kalshi markets users searched for or viewed, the event contracts they selected, whether they selected “Yes” or “No,” whether they bought or sold, the dollar amount or contract quantity associated with the trade, order identifiers, user or account identifiers, URLs, page titles, button

clicks, and other activity reflecting the substance of their interactions with Kalshi's Digital Platforms.

156. Kalshi intentionally embedded, configured, activated, or permitted third-party tracking technologies to operate on its Digital Platforms.

157. These tracking technologies operate in real time. When a user loads a Kalshi page, Kalshi's Website sends code to the user's browser. That code instructs the browser to load additional third-party scripts and to transmit information to third-party servers as the user navigates the Website, searches for markets, clicks buttons, enters information, reviews order screens, and places event-contract trades.

158. As a result, an "interception," within the meaning of Fla. Stat. § 934.02(3), occurs during transmission. While Plaintiffs and Florida Subclass members communicated with Kalshi's Digital Platforms, Kalshi's tracking code caused their browsers or devices to send parallel transmissions to third-party servers. Those transmissions occurred contemporaneously with, or substantially contemporaneously with, the users' communications with Kalshi—not merely after the communications had ended or after the information had come to rest in storage.

159. The third-party tracking technologies acquired the contents of Plaintiffs and Florida Subclass members' communications through the use of electronic, mechanical, or other devices, including the code, pixels, scripts, SDKs, cookies, browser identifiers, and tag-management tools that Kalshi deployed or permitted to operate on the Digital Platforms.

160. The third-party recipients of these communications were independent entities that, upon information and belief: operated their own data collection and monetization infrastructures; used the intercepted data for their own commercial purposes, including targeted advertising and

profiling; and were not necessary intermediaries to the transmission of communications between Plaintiffs and Defendants.

161. Defendants knowingly and intentionally procured and enabled these third parties to intercept Plaintiffs' communications by embedding and activating the third-party trackers on its Digital Platforms.

162. Defendants' conduct was not passive, accidental, or incidental. Kalshi affirmatively designed or permitted an architecture in which users' browsers communicated simultaneously with Kalshi and third-party tracking vendors during sensitive digital interactions, including market searches, account interactions, order-flow activity, and event-contract trades.

163. Plaintiffs and Florida Subclass members did not consent to the interception, disclosure, or use of their electronic communications, PII, trading activity, or sensitive activity by Kalshi's third-party advertising, analytics, attribution, social media, or marketing-technology partners.

164. Defendants cannot establish implied consent because it failed to provide clear and conspicuous notice of the challenged interceptions before the trackers fired. Kalshi did not require users to review or affirmatively agree to its Privacy Policy before third-party tracking began; did not disclose in a clear, prominent, and specific manner that third parties would receive information revealing users' market searches, trade selections, "Yes" or "No" positions, buy/sell activity, dollar amounts, order-flow activity, or trading behavior; and did not provide a straightforward mechanism for users to decline or withdraw consent before their communications were intercepted.

165. Defendants' generic, buried, or inconspicuous references to legal terms, cookies, analytics, or advertising were insufficient to obtain prior consent from all parties to the communications. A reasonable user would not understand from Kalshi's sign-up flow or Digital

Platform design that third-party advertising and analytics companies would receive real-time information revealing the user's sensitive event-contract trading activity.

166. Defendants' own Rulebook further undermines any assertion that Plaintiffs and Florida Subclass members impliedly consented to the challenged interceptions. Rule 11.1(e) provides that Kalshi may not condition access to its exchange on a participant's consent to the use of Personal Information or Proprietary Data for business or marketing purposes and may not use such information for those purposes unless the participant has "clearly consented." Yet Kalshi did not provide users with a separate, optional, or clearly described choice concerning the marketing use or third-party acquisition of their information.

167. Instead, Kalshi bundled generalized data-use language into legal documents that users were required to accept to trade, without specifically disclosing that independent advertising and analytics companies would contemporaneously receive identifiable information revealing users' market searches, event-contract selections, "Yes" or "No" positions, buy/sell activity, dollar amounts, and completed trades. A user's decision to proceed through that mandatory sign-up process did not constitute the clear, specific, and voluntary consent contemplated by Kalshi's own Rulebook and did not authorize the real-time third-party interceptions alleged herein.

168. Defendants further intentionally disclosed and used the contents of Plaintiffs' communications, knowing or having reason to know that such information was obtained through interception, in violation of Fla. Stat. § 934.03(1)(c)–(d). Defendants used the intercepted information for commercial purposes, including advertising, analytics, attribution, retargeting, audience creation, marketing optimization, user acquisition, and increasing engagement with the Digital Platforms.

169. Defendants' violations were willful, knowing, and undertaken for commercial gain, entitling Plaintiffs and Florida Subclass members to punitive damages.

170. Pursuant to Fla. Stat. § 934.10, Plaintiffs and Florida Subclass members seek: statutory damages; actual damages; punitive damages; and reasonable attorneys' fees and costs.

COUNT II
**VIOLATION OF THE PENNSYLVANIA WIRETAPPING AND ELECTRONIC
SURVEILLANCE CONTROL ACT, 18 PA. C.S. § 5701, et seq.**
(On behalf of the Pennsylvania Subclass)

171. Plaintiff Nicholas Ross re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein, and brings this Count individually and on behalf of the Pennsylvania Subclass against the Defendants.

172. The Pennsylvania Wiretap Act ("WESCA") prohibits: (1) the intentional interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703

173. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Pennsylvania Wiretap Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of \$100/day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

174. “Intercept” means any “[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.” 18 Pa. Cons. Stat. § 5702.

175. “Contents” means “any information concerning the substance, purport, or meaning of that communication.” 18 Pa. Cons. Stat. § 5702.

176. “Person” means “any individual, partnership, association, joint stock company, trust or corporation.” 18 Pa. Cons. Stat. § 5702.

177. “Electronic Communication” means “[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system.” 18 Pa. Cons. Stat. § 5702.

178. Plaintiff Nicholas Ross’s and Pennsylvania Subclass members’ communications with Kalshi’s Website are electronic communications under WESCA because they involved the electronic transfer of data, signals, writings, requests, responses, searches, form-field entries, page views, button clicks, order-flow information, and event-contract trade information between users’ devices or browsers and Kalshi’s Website.

179. Because Kalshi is a corporation, it is a person under the Pennsylvania Wiretap Tracking Act.

180. Defendants’ tracking technologies qualify as “electronic, mechanical or other device[s]” under WESCA. The tracking code, JavaScript, pixels, tags, cookies, SDKs, browser identifiers, and tag-management tools Kalshi deployed or permitted to operate on the Website were used to acquire the contents of Plaintiff Nicholas Ross’s and Pennsylvania Subclass members’ electronic communications.

181. The intercepted data revealed the substance, purport, and meaning of Plaintiff Nicholas Ross's and Pennsylvania Subclass members' communications with Kalshi. This information included, upon information and belief, the specific Kalshi markets users searched for or viewed, the event contracts they selected, whether they selected "Yes" or "No," whether they bought or sold, the amount or quantity associated with a trade, order-flow activity, trade-placement activity, buttons clicked, URLs, page titles, account or user identifiers, device identifiers, and other activity data.

182. In the context of Kalshi's Website, URLs, page titles, event names, query parameters, order-flow fields, and button-click events carry substantive meaning. They can reveal that a user researched a particular event contract, selected a side of the contract, chose to buy or sell, placed or attempted to place a trade, and risked money on a particular real-world outcome.

183. The interception occurred contemporaneously with transmission. When Plaintiff Nicholas Ross and Pennsylvania Subclass members communicated with Kalshi's Website, Kalshi's embedded tracking technologies caused their browsers or devices to send parallel communications to third-party servers in real time or near-real time.

184. Defendants intentionally procured these interceptions. Kalshi selected, embedded, configured, activated, or permitted third-party tracking technologies on its Website and caused those technologies to acquire and transmit users' communications and sensitive Website activity to third-party advertising, analytics, attribution, social media, and marketing-technology companies.

185. Defendants' conduct was intentional and not incidental. Kalshi affirmatively integrated the trackers into its Website architecture and trading flow, including pages and events associated with searches, market views, account interactions, order-flow activity, and event-

contract trades. Kalshi knew or should have known that these trackers would transmit user communications and activity data to third-party servers.

186. The third-party recipients were independent entities that were not necessary intermediaries to the communications between Plaintiff Nicholas Ross, Pennsylvania Subclass members, and Kalshi. Upon information and belief, they used the intercepted information for their own purposes, including advertising, analytics, attribution, retargeting, audience creation, profiling, and marketing optimization.

187. Plaintiff Nicholas Ross and Pennsylvania Subclass members had a reasonable expectation that their communications with Kalshi concerning event-contract trading, account activity, financial behavior, and market selections would not be intercepted by third-party advertising, analytics, social media, or marketing-technology companies.

188. Plaintiff Nicholas Ross and Pennsylvania Subclass members did not consent to the interception, disclosure, or use of their electronic communications, PII, trading activity, or sensitive Website activity by Kalshi's third-party tracking partners.

189. Kalshi cannot establish implied consent because it failed to provide clear and conspicuous notice of the challenged tracking before the interceptions occurred. Kalshi did not require users to affirmatively agree to a disclosure authorizing third-party tracking of sensitive event-contract trading activity, did not provide just-in-time notice before transmitting trade-related information, and did not offer a meaningful opportunity to decline or revoke consent before the trackers fired.

190. Defendants' inconspicuous or generic references to legal terms, cookies, analytics, or advertising did not put Plaintiff Nicholas Ross or Pennsylvania Subclass members on notice that third-party trackers would receive information revealing their Kalshi market searches, event-

contract selections, “Yes” or “No” positions, buy/sell activity, dollar amounts, order-flow activity, visit frequency, or trading behavior.

191. Defendants’ own Rulebook further undermines any assertion that Plaintiff Ross and Pennsylvania Subclass members impliedly consented to the challenged interceptions. Rule 11.1(e) provides that Kalshi may not condition access to its exchange on a participant’s consent to the use of Personal Information or Proprietary Data for business or marketing purposes and may not use such information for those purposes unless the participant has “clearly consented.” Yet Kalshi did not provide users with a separate, optional, or clearly described choice concerning the marketing use or third-party acquisition of their information.

192. Instead, Kalshi bundled generalized data-use language into legal documents that users were required to accept to trade, without specifically disclosing that independent advertising and analytics companies would contemporaneously receive identifiable information revealing users’ market searches, event-contract selections, “Yes” or “No” positions, buy/sell activity, dollar amounts, and completed trades. A user’s decision to proceed through that mandatory sign-up process did not constitute the clear, specific, and voluntary consent contemplated by Kalshi’s own Rulebook and did not authorize the real-time third-party interceptions alleged herein.

193. Defendants intentionally disclosed and used the contents of Plaintiff Nicholas Ross’s and Pennsylvania Subclass members’ communications, knowing or having reason to know that the information was obtained through interception. Kalshi used the information for advertising, analytics, attribution, retargeting, audience creation, marketing optimization, user acquisition, and increasing engagement with Kalshi’s Website.

194. Defendants’ violations were intentional, knowing, willful, and undertaken for commercial gain. Plaintiff Nicholas Ross and Pennsylvania Subclass members suffered injury,

including invasion of privacy, loss of control over their communications and data, unauthorized disclosure of sensitive trading activity, and loss of the value of their personal information and Website activity.

195. Under the Pennsylvania Wiretap Act, Plaintiff and Class Members seek: (1) actual damages, not less than liquidated damages computed at the rate of \$100/day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

COUNT III
UNJUST ENRICHMENT
(On behalf of the Nationwide Class)

196. Plaintiffs re-allege and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein and bring this claim on behalf of themselves and the Nationwide class.

197. Plaintiffs and Class Members conferred valuable benefits on Kalshi by using the Website and providing Kalshi with access to their PII, communications, browsing activity, market searches, event-contract interests, order-flow activity, trading activity, financial behavior, device identifiers, location information, and other sensitive data.

198. Kalshi knowingly accepted and retained those benefits. Kalshi collected, used, disclosed, and monetized Plaintiffs' and Class Members' data, including by transmitting it to third-party advertising, analytics, attribution, social media, and marketing-technology companies.

199. The data at issue has independent economic value. It identifies or can be linked to Plaintiffs and Class Members and reveals sensitive information about their wagering-like activity, including the markets they viewed, the outcomes they predicted, whether they selected "Yes" or

“No,” the amount of money they risked, the frequency and timing of their visits, and their trading patterns.

200. Kalshi received direct economic and strategic benefits from Plaintiffs’ and Class Members’ data. Upon information and belief, those benefits included targeted advertising, retargeting, conversion attribution, audience creation, lookalike modeling, analytics, marketing optimization, reduced customer-acquisition costs, increased user engagement, increased trading activity, and increased revenue.

201. Kalshi’s benefit did not require a direct cash sale of Plaintiffs’ and Class Members’ data. The advertising, analytics, attribution, audience-building, retargeting, and optimization services Kalshi received in exchange for or through the disclosure of Plaintiffs’ and Class Members’ data constitute valuable commercial benefits.

202. Plaintiffs and Class Members did not knowingly authorize Kalshi to disclose, license, or otherwise monetize their PII, communications, trading activity, or sensitive activity for Kalshi’s commercial gain. Nor were Plaintiffs and Class Members compensated for the value Kalshi extracted from their data.

203. Had Plaintiffs and Class Members known that Kalshi would disclose their PII, communications, and sensitive Digital Platform activity to third-party advertising, analytics, attribution, social media, and marketing-technology companies, they would not have used the Digital Platforms, would not have provided their data to Kalshi, would have taken steps to prevent the disclosure, or would have demanded compensation for the use of their data.

204. Kalshi was aware that Plaintiffs and Class Members reasonably expected their sensitive Digital Platform activity, event-contract trading activity, financial behavior, and

communications with Kalshi to remain private and not to be disclosed or exploited for commercial gain without informed consent.

205. Kalshi's retention of the benefits derived from Plaintiffs' and Class Members' data is inequitable and unjust because Kalshi obtained those benefits through undisclosed and unauthorized tracking and disclosure practices, while Plaintiffs and Class Members bore the privacy harms, loss of control, and loss of economic value associated with the disclosure of their data.

206. Plaintiffs and Class Members suffered injury as a result of Kalshi's unjust enrichment, including invasion of privacy, loss of control over their PII and sensitive activity, deprivation of the economic value of their data, and unauthorized commercialization of their trading and behavioral information.

207. Equity and good conscience require that Defendants disgorge the profits, benefits, savings, revenues, and other value it obtained from its unauthorized collection, use, disclosure, and monetization of Plaintiffs' and Class Members' data. Plaintiffs and Class Members seek restitution, disgorgement, imposition of a constructive trust where appropriate, and all other equitable relief the Court deems just and proper.

COUNT IV
CONSTRUCTIVE BAILMENT
(On behalf of the Nationwide Class)

208. Plaintiffs re-allege and incorporate by reference the allegations above as if fully set forth herein and bring this claim on behalf of themselves and the Nationwide Class.

209. A constructive bailment arises when one party obtains possession or control of another's property under circumstances that impose a duty to safeguard, preserve, return, delete, or account for that property, even absent an express bailment agreement.

210. Courts have recognized, at least at the pleading stage, that bailment principles may apply to personal information or electronic data where a Defendant accepts custody or control over data under circumstances reflecting a shared understanding that the information will remain confidential. *See, e.g., Wallace v. Health Quest Sys., Inc.*, 2021 WL 1109727, at *13–14 (S.D.N.Y. Mar. 23, 2021); *Krupa v. TIC Int’l Corp.*, 2023 WL 143140, at *4–5 (S.D. Ind. Jan. 10, 2023).

211. Plaintiffs and Class Members entrusted Kalshi with their PII and sensitive activity for the limited purpose of creating and maintaining Kalshi accounts, verifying their identities, funding their accounts, enabling event-contract trading, complying with applicable legal obligations, and providing Kalshi’s trading-related services.

212. This information included, among other things, Plaintiffs’ and Class Members’ names, email addresses, telephone numbers, dates of birth, residential addresses, identity-verification information, financial information, account identifiers, device identifiers, location information, Digital Platform activity, market searches, event-contract interests, order-flow activity, trading activity, and related communications with Kalshi.

213. Kalshi accepted possession, custody, and control over Plaintiffs’ and Class Members’ PII and sensitive activity as a condition of using its services, stored and processed that information in its systems, associated that information with users’ accounts and devices, and controlled whether and how the information would be collected, used, protected, disclosed, deleted, or transmitted to third parties.

214. Plaintiffs and Class Members did not transfer ownership of their PII, communications, Digital Platform activity, or sensitive trading information to Kalshi. Rather, they entrusted that information to Kalshi for the limited purpose of receiving Kalshi’s services and reasonably expected that Kalshi would safeguard the information, use it only for authorized

purposes, and not disclose it to unrelated third-party advertising, analytics, attribution, social media, or marketing-technology companies without informed consent.

215. Under these circumstances, Kalshi became a constructive bailee of Plaintiffs' and Class Members' PII and sensitive Digital Platform activity. A constructive bailment arises when Kalshi, as is the case here, takes lawful possession of the property of another and has a duty to account for that property, without intending to appropriate it.

216. Constructive bailments do not require an express assumption of duties and may arise from the bare fact of the thing coming into the actual possession and control of a person fortuitously or by mistake as to the duty or ability of the recipient to affect the purpose contemplated by the absolute owner.

217. During the bailment, Kalshi owed a duty to Plaintiffs and Class Members a duty to exercise reasonable care, diligence, and prudence in safeguarding their PII, communications, Digital Platform activity, and sensitive trading information. Kalshi also owed Plaintiffs and Class Members a duty to use the information only for the limited purposes for which it was entrusted and to prevent unauthorized interception, disclosure, access, misuse, or commercial exploitation.

218. Kalshi breached its duty as constructive bailee by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class Members' PII and sensitive Digital Platforms activity. Among other things, Kalshi embedded, configured, activated, or permitted third-party tracking technologies on the Digital Platforms that collected and transmitted Plaintiffs' and Class Members' information to third parties without their knowledge, consent, or authorization.

219. Kalshi further breached its duty to safeguard Plaintiffs' and Class Members' PII by failing to notify them individually in a timely and accurate manner that their PII, Digital Platform

activity, and sensitive trading information had been disclosed to third parties without Plaintiffs' and Class Members' knowledge, consent or explicit authorization.

220. Kalshi's disclosure and transmission of Plaintiffs' and Class Members' information exceeded the limited purpose for which Plaintiffs and Class Members entrusted their information to Kalshi. Plaintiffs and Class Members did not entrust their PII and sensitive Digital Platform activity to Kalshi so that Kalshi could disclose, license, monetize, or otherwise exploit that information for advertising, analytics, profiling, retargeting, audience creation, or marketing optimization.

221. As a direct and proximate result of Kalshi's breach of its constructive bailment duties, Plaintiffs and Class Members have suffered compensable damages, including loss of control over their PII and sensitive Digital Platform activity, invasion of privacy, deprivation of the value of their data, unauthorized commercialization of their information, disclosure of sensitive betting and trading activity, and the present and continuing risk that their information will be further used, retained, combined, analyzed, profiled, or disseminated by third parties, that were reasonably foreseeable to Kalshi.

DEMAND FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class and Subclasses, respectfully request that the Court:

a. Certify the Nationwide Class, Florida Subclass, and Pennsylvania Subclass under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3); appoint Adrian Vazquez and Alexander Foley as representatives of the Nationwide Class and the Florida Subclass and Nicholas Ross for the Pennsylvania Subclass; and appoint undersigned counsel as Class Counsel;

b. Declare that Defendants' conduct violated the Florida Security of Communications Act, Fla. Stat. §§ 934.01 et seq., and the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701 et seq;

c. Declare that Defendants was unjustly enriched by its unauthorized collection, use, disclosure, and monetization of Plaintiffs' and Class Members' PII, trading activity, and sensitive Digital Platform activity;

d. Declare that Defendants breached its duties as constructive bailee by failing to safeguard Plaintiffs' and Class Members' PII, trading activity, and sensitive Digital Platform activity, and by disclosing or permitting the disclosure of that information to third parties without informed consent;

e. Award actual, compensatory, and nominal damages, and statutory damages as available under each claim, including Fla. Stat. § 934.10 and 18 Pa. Cons. Stat. § 5725(a);

f. Award punitive damages to the extent permitted by law;

g. Order restitution, disgorgement, and/or imposition of a constructive trust over all profits, revenues, savings, benefits, or other value Defendants obtained from the challenged conduct;

h. Award appropriate injunctive relief, including an order requiring Defendants to cease the challenged tracking and disclosure practices; remove or disable unlawful third-party tracking technologies; obtain valid, informed, and affirmative consent before disclosing users' PII, communications, trading activity, or sensitive Digital Platform activity to third parties; provide clear and conspicuous notice of third-party tracking; implement reasonable privacy safeguards; and delete, retrieve, or prevent further use of improperly disclosed data where feasible;

- i. Award appropriate declaratory relief concerning Defendants' past and ongoing privacy practices;
- j. Award pre- and post-judgment interest, attorneys' fees, expert fees, and costs; and
- k. Grant such other relief as the Court deems just and proper.

JURY TRIAL DEMAND

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiffs, on behalf of themselves and the proposed Class and Subclasses, demand a jury trial as to all issues so triable.

DATED: July 9, 2026

Respectfully Submitted,

/s/ Jennifer S. Czeisler

Jennifer S. Czeisler*

Edward W. Ciolko*

Jennifer J. Sosa

STERLINGTON, PLLC

228 Park Avenue South, Suite 97956,

New York, New York 10003

Tel.: (212) 433-2993

jen.czeisler@sterlingtonlaw.com

edward.ciolko@sterlingtonlaw.com

jenn.sosa@sterlingtonlaw.com

**LITE DEPALMA GREENBERG &
AFANADOR, LLC**

Joseph J. DePalma*

Catherine B. Derenze*

570 Broad St., Suite 1201

Newark, New Jersey 07102

Tel: (973) 623-3000

jdepalma@litedepalma.com

cderenze@litedepalma.com

*Attorneys for Plaintiffs
and the Proposed Class*

*Pro Hac Vice Forthcoming