

1 STEVEN M. NATHAN, SBN 153250
2 HAUSFELD LLP
3 33 Whitehall Street
4 Fourteenth Floor
5 New York, NY 10034
6 Tel: (646) 357-1100
7 Fax: (212) 202-4322
8 snathan@hausfeld.com

9 *Attorneys for Plaintiff*
10 *(additional counsel on signature page)*

11 **IN THE UNITED STATES DISTRICT COURT**
12 **FOR THE SOUTHERN DISTRICT OF CALIFORNIA**

13 KAYLA MANDENG, individually and
14 on behalf of all others similarly situated,

15 Plaintiff,

16 vs.

17 SPIRIT AIRLINES, INC.
18 Defendant.

Case No.:

CLASS ACTION COMPLAINT
DEMAND FOR JURY TRIAL

19 **COMPLAINT - CLASS ACTION**

20 Plaintiff, Kayla Mandeng (“Plaintiff”), individually and on behalf of all others
21 similarly situated, hereby files this class action complaint against Defendant Spirit
22 Airlines, Inc. (“Spirit”), and in support thereof alleges the following:

23 **INTRODUCTION**

24 1. This is a class action brought against Spirit for wiretapping the electronic
25 communications of visitors to its website, www.spirit.com. Spirit procures third-party
26 vendors, such as FullStory, to embed snippets of JavaScript computer code (“Session
27 Replay Code”) on Spirit’s website, which then deploys on each website visitor’s
28 internet browser for the purpose of intercepting and recording the website visitor’s
electronic communications with the Spirit website, including their mouse movements,

1 clicks, keystrokes (such as text being entered into an information field or text box),
2 URLs of web pages visited, and/or other electronic communications in real-time
3 (“Website Communications”). These third-party vendors (collectively, “Session
4 Replay Providers”) create and deploy the Session Replay Code at Spirit’s request.

5 2. After intercepting and capturing the Website Communications, Spirit and
6 the Session Replay Providers use those Website Communications to recreate website
7 visitors’ entire visit to www.spirit.com. The Session Replay Providers create a video
8 replay of the user’s behavior on the website and provide it to Spirit for analysis. Spirit’s
9 procurement of the Session Replay Providers to secretly deploy the Session Replay
10 Code results in the electronic equivalent of “looking over the shoulder” of each visitor
11 to the Spirit website for the entire duration of their website interaction.

12 3. Spirit’s conduct violates the California Invasion of Privacy Act, Cal.
13 Penal Code § 630 *et seq.* and constitutes the torts of invasion of the privacy rights and
14 intrusion upon seclusion of website visitors.

15 4. Plaintiff brings this action individually and on behalf of a class of all
16 persons in California whose Website Communications were intercepted through
17 Spirit’s procurement and use of Session Replay Code embedded on the webpages of
18 www.spirit.com and seeks all civil remedies provided under the causes of action,
19 including but not limited to compensatory, statutory, and/or punitive damages, and
20 attorneys’ fees and costs.

21 **PARTIES**

22 5. Plaintiff Kayla Mandeng is a citizen of the State of California, and at all
23 times relevant to this action, resided and was domiciled in the State of California.

24 6. Defendant Spirit is a corporation organized under the laws of Delaware,
25 and its principal place of business is located in Miramar, Florida. Spirit is a citizen of
26 Florida.

1 **JURISDICTION AND VENUE**

2 7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §
3 1332(d)(2)(A) because this case is a class action where the aggregate claims of all
4 members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and
5 costs, there are 100 or more members of the proposed class, and at least one member
6 of the proposed class, including Plaintiff, is a citizen of a state different than Defendant.

7 8. This Court has personal jurisdiction over Defendant because a substantial
8 part of the events and conduct giving rise to Plaintiff's claims occurred in California.
9 Further, Defendant purposefully directed its activities to California, consummated
10 transactions in California and purposefully availed itself of the privilege of conducting
11 activities in California thereby invoking the benefits and protections of California law.
12 Specifically, Plaintiff, while in California, accessed and viewed the www.spirit.com
13 website, reviewed flights to and/or from California airports and booked airline tickets
14 from an airport in California. Further, Plaintiff paid for the airline tickets through the
15 www.spirit.com website.

16 9. The privacy violations complained of herein resulted from Defendant's
17 purposeful and tortious acts directed towards citizens of California while they were
18 located within California. At all relevant times, Defendant knew that its practices
19 would directly result in the collection of information from California citizens while
20 those citizens browse www.spirit.com and book (and pay for) Spirit airline tickets.
21 Defendant chose to avail itself of the business opportunities of marketing and selling
22 its goods and services in California and collecting real-time data from website visit
23 sessions initiated by California residents while located in California, and the claims
24 alleged herein arise from those activities.

25 10. Spirit also knows that many users visit and interact with Spirit's websites
26 while they are physically present in California. Both desktop and mobile versions of
27 Spirit's website allow a user to search for available flights from the user's current
28 location, as furnished by the location-determining tools of the device the user is using

1 or by the user’s IP address (*i.e.*, without requiring the user to manually input an
2 address). Users’ employment of automatic location services in this way means that
3 Spirit is continuously made aware that its website is being visited by people located in
4 California, and that such website visitors are being wiretapped in violation of California
5 statutory and common law. Additionally, Spirit directly engages in commerce in
6 California by offering flights to and from California airports. Through its website,
7 www.spirit.com, Spirit identifies 6 airports in California which it serves: Oakland, Los
8 Angeles, San Diego, Burbank, Orange County and Sacramento.¹

9 11. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action
10 because a substantial part of the events, omissions, and acts giving rise to the claims
11 herein occurred in this District.

12 FACTUAL ALLEGATIONS

13 **A. Website User and Usage Data Have Immense Economic Value.**

14 12. The “world’s most valuable resource is no longer oil, but data.”²

15 13. Earlier this year, Business News Daily reported that some businesses
16 collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs),
17 engagement data (*i.e.*, how consumers interact with a business’s website, applications,
18 and emails), behavioral data (*i.e.*, customers’ purchase histories and product usage
19 information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.³
20 This information is valuable to companies because they can use this data to improve
21 customer experiences, refine their marketing strategies, capture data to sell it, and even
22 to secure more sensitive consumer data.⁴

23
24 ¹ See www.spirit.com/en/route-map.

25 ² *The world’s most valuable resource is no longer oil, but data*, The Economist (May
26 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data>.

27 ³ Max Freedman, *How Businesses Are Collecting Data (And What They’re Doing With It)*, Business News Daily (Aug. 5, 2022), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>.

28 ⁴ *Id.*

1 14. In a consumer-driven world, the ability to capture and use customer data
2 to shape products, solutions, and the buying experience is critically important to a
3 business's success. Research shows that organizations who "leverage customer
4 behavior insights outperform peers by 85 percent in sales growth and more than 25
5 percent in gross margin."⁵

6 15. In 2013, the Organization for Economic Cooperation and Development
7 ("OECD") even published a paper entitled "Exploring the Economics of Personal Data:
8 A Survey of Methodologies for Measuring Monetary Value."⁶ In this paper, the OECD
9 measured prices demanded by companies concerning user data derived from "various
10 online data warehouses."⁷

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

17 **B. Website Users Have a Reasonable Expectation of Privacy in Their**
18 **Interactions with Websites.**

19 17. Consumers are skeptical and are wary about their data being collected. A
20 report released by KPMG shows that "a full 86% of the respondents said they feel a
21
22
23

24 ⁵ Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing*
25 *value from your customer data*, McKinsey (Mar. 15, 2017),
[https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-](https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data)
[value-from-your-customer-data](https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data).

26 ⁶ Exploring the Economics of Personal Data: A Survey of Methodologies for
27 Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013),
<https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

28 ⁷ *Id.* at 25.

⁸ *Id.*

1 growing concern about data privacy, while 78% expressed fears about the amount of
2 data being collected.”⁹

3 18. Another recent paper also indicates that most website visitors will assume
4 their detailed interactions with a website will only be used by the website and not be
5 shared with a party they know nothing about.¹⁰ As such, website visitors reasonably
6 expect that their interactions with a website should not be released to third parties
7 unless explicitly stated.¹¹

8 19. Privacy polls and studies show that a majority of Americans consider one
9 of the most important privacy rights to be the need for an individual’s affirmative
10 consent before a company collects and shares its customers’ data.

11 20. A recent study by Consumer Reports shows that 92% of Americans
12 believe that internet companies and websites should be required to obtain consent
13 before selling or sharing consumers’ data, and the same percentage believe internet
14 companies and websites should be required to provide consumers with a complete list
15 of the data that has been collected about them.¹²

16 21. Moreover, according to a study by Pew Research Center, a majority of
17 Americans, approximately 79%, are concerned about how data is collected about them
18 by companies.¹³

19
20 ⁹ Lance Whitney, *Data privacy is a growing concern for more consumers*,
TechRepublic (Aug. 17, 2021), <https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/>.

21 ¹⁰ *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns*
22 *Towards Privacy and Online Tracking*, CUJO (May 26, 2020),
23 <https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html>.

24 ¹¹ Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A*
Privacy Analysis, *The Information Society*, 38:4, 257, 258 (2022).

25 ¹² *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New*
26 *Survey Finds*, *Consumer Reports* (May 11, 2017),
27 <https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

28 ¹³ *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over*
Their Personal Information, *Pew Research Center*, (Nov. 15, 2019),

1 22. Users act consistently with their expectation of privacy. Following a new
2 rollout of the iPhone operating software—which asks users for clear, affirmative
3 consent before allowing companies to track users—85 percent of worldwide users and
4 94 percent of U.S. users chose not to allow such tracking.¹⁴

5 **C. How Session Replay Code Works.**

6 23. Session Replay Code, such as that implemented on www.spirit.com,
7 enables website operators to record, save, and replay website visitors' interactions with
8 a given website. The clandestinely deployed code provides online marketers and
9 website designers with insights into the user experience by recording website visitors
10 “as they click, scroll, type or navigate across different web pages.”¹⁵

11 24. While Session Replay Code is utilized by websites for some legitimate
12 purposes, it goes well beyond normal website analytics when it comes to collecting the
13 actual contents of communications between website visitors and websites. Unlike other
14 online advertising tools, Session Replay Code allows a website to capture and record
15 nearly every action a website visitor takes while visiting the website, including actions
16 that reveal the visitor's personal or private sensitive data, sometimes even when the
17 visitor does not intend to submit the data to the website operator, or has not finished
18 submitting the data to the website operator.¹⁶ As a result, website visitors “aren't just
19 sharing data with the [web]site they're on . . . but also with an analytics service that
20 may be watching over their shoulder.”¹⁷

21
22
23 <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/>.

24 ¹⁴ Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021),
25 <https://www.wired.co.uk/article/apple-ios14-facebook>.

26 ¹⁵ Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), <https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/>.

27 ¹⁶ *Id.*

28 ¹⁷ Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), <https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0>.

1 25. Session Replay Code works by inserting computer code into the various
2 event handling routines that web browsers use to receive input from users, thus
3 intercepting the occurrence of actions the user takes. When a website delivers Session
4 Replay Code to a user’s browser, the browser will follow the code’s instructions by
5 sending responses in the form of “event” data to a designated third-party server.
6 Typically, the server receiving the event data is controlled by the third-party entity that
7 wrote the Session Replay Code, rather than the owner of the website where the code is
8 installed.

9 26. The types of events captured by Session Replay Code vary by specific
10 product and configuration, but in general are wide-ranging and can encompass virtually
11 every user action, including all mouse movements, clicks, scrolls, zooms, window
12 resizes, keystrokes, text entry, and numerous other forms of a user’s navigation and
13 interaction through the website. In order to permit a reconstruction of a user’s visit
14 accurately, the Session Replay Code must be capable of capturing these events at
15 hyper-frequent intervals, often just milliseconds apart. Events are typically
16 accumulated and transmitted in blocks periodically throughout the user’s website
17 session, rather than after the user’s visit to the website is finished.

18 27. Unless specifically masked through configurations chosen by the website
19 owner, some visible contents of the website may also be transmitted to the Session
20 Replay Provider.

21 28. Once the events from a user session have been recorded by a Session
22 Replay Code, a website operator can view a visual reenactment of the user’s visit
23 through the Session Replay Provider, usually in the form of a video, meaning “[u]nlike
24 typical analytics services that provide aggregate statistics, these scripts are intended for
25 the recording and playback of individual browsing sessions.”¹⁸

26
27 ¹⁸ Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay*
28 *scripts*, Freedom to Tinker (Nov. 15, 2017), <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>.

1 29. Because most Session Replay Codes will by default indiscriminately
2 capture the maximum range of user-initiated events and content displayed by the
3 website, researchers have found that a variety of highly sensitive information can be
4 captured in event responses from website visitors, including medical conditions, credit
5 card details, and other personal information displayed or entered on webpages.¹⁹

6 30. Most alarming, Session Replay Code may capture data that the user did
7 not even intentionally transmit to a website during a visit, and then make that data
8 available to website owners when they access the session replay through the Session
9 Replay Provider. For example, if a user writes information into a text form field, but
10 then chooses not to click a “submit” or “enter” button on the website, the Session
11 Replay Code may nevertheless cause the non-submitted text to be sent to the designated
12 event-response-receiving server before the user deletes the text or leaves the page. This
13 information will then be viewable to the website owner when accessing the session
14 replay through the Session Replay Provider.

15 31. Session Replay Code does not necessarily anonymize user sessions,
16 either.

17 32. First, if a user’s entry of personally identifying information is captured in
18 an event response, that data will become known and visible to both the Session Replay
19 Provider and the website owner.

20 33. Second, if a website displays user account information to a logged-in user,
21 that content may be captured by Session Replay Code.

22 34. Third, some Session Replay Providers explicitly offer website owners
23 cookie functionality that permits linking a session to an identified user, who may be
24 personally identified if the website owner has associated the user with an email address
25 or username.²⁰

26
27 _____
28 ¹⁹ *Id.*

²⁰ *Id.*; see also *FS.identify – Identifying users*, FullStory, <https://help.fullstory.com/hc/en-us/articles/360020828113>, (last visited Sep. 8, 2022).

1 35. Session Replay Providers often create “fingerprints” that are unique to a
2 particular user’s combination of computer and browser settings, screen configuration,
3 and other detectable information. The resulting fingerprint, which is often unique to a
4 user and rarely changes, are collected across all sites that the Session Replay Provider
5 monitors.

6 36. When a user eventually identifies themselves to one of these websites
7 (such as by filling in a form), the provider can then associate the fingerprint with the
8 user identity and can then back-reference all of that user’s other web browsing across
9 other websites previously visited, including on websites where the user had intended
10 to remain anonymous—even if the user explicitly indicated that they would like to
11 remain anonymous by enabling private browsing.

12 37. In addition to the privacy invasions caused by the diversion of user
13 communications with websites to third-party Session Replay Providers, Session Replay
14 Code also exposes website visitors to identity theft, online scams, and other privacy
15 threats.²¹ Indeed, “[t]he more copies of sensitive information that exist, the broader the
16 attack surface, and when data is being collected [] it may not be stored properly or
17 have standard protections” increasing “the overall risk that data will someday publicly
18 leak or be breached.”²²

19 38. The privacy concerns arising from Session Replay Code are not
20 theoretical or imagined. The CEO and founder of LOKKER, a provider of data privacy
21 and compliance solutions has said “[consumers] should be concerned” about the use of
22 Session Replay Code because “they won’t know these tools are operating ‘behind the
23
24
25

26 ²¹ Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov.
27 16, 2017), <https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720>.

28 ²² Lily Hay Newman, *Covert ‘Replay Sessions’ Have Been Harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), <https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/>.

1 scenes’ of their site visit” and “even if the company disclosed that they are using these
2 tools, consumers wouldn’t likely be able to opt-out and still use the site.”²³

3 39. Indeed, the news is replete with examples of the dangers of Session
4 Replay Code. For example, in 2019, the App Analyst, a mobile expert who writes about
5 his analyses of popular apps, found that Air Canada’s iPhone app wasn’t properly
6 masking the session replays they were sent, exposing unencrypted credit card data and
7 password information.²⁴ This discovery was made just weeks after Air Canada said its
8 app had a data breach, exposing 20,000 profiles.²⁵

9 40. Further, multiple companies have removed Session Replay Code from
10 their websites after it was discovered the Session Replay Code captured highly
11 sensitive information. For instance, in 2017, Walgreens stopped sharing data with a
12 Session Replay Provider after it was discovered that the Session Replay provider
13 gained access to website visitors’ sensitive information.²⁶ Indeed, despite Walgreens’
14 extensive use of manual redactions for displayed and inputted data, the Session Replay
15 Provider still gained access to full names of website visitors, their medical conditions,
16 and their prescriptions.²⁷

17 41. Following the Walgreens incident, Bonobos, a men’s clothing retailer,
18 announced that it was eliminating data sharing with a Session Replay Provider after it
19 was discovered that the Session Replay Provider captured credit card details, including
20 the cardholder’s name and billing address, and the card’s number, expiration, and
21 security code from the Bonobos’ website.²⁸

22 ²³ Mark Huffner, *Is ‘session replay software’ a privacy threat or just improving your*
23 *web experience*, Consumer Affairs (Oct. 25, 2022),
24 [https://www.consumeraffairs.com/news/is-session-replay-software-a-privacy-threat-](https://www.consumeraffairs.com/news/is-session-replay-software-a-privacy-threat-or-just-improving-your-web-experience-102522.html)
[or-just-improving-your-web-experience-102522.html](https://www.consumeraffairs.com/news/is-session-replay-software-a-privacy-threat-or-just-improving-your-web-experience-102522.html).

25 ²⁴ Zach Whittaker, *Many Popular iPhone Apps Secretly Record Your Screen Without*
Asking, TechCrunch (Feb. 6, 2019), [https://techcrunch.com/2019/02/06/iphone-](https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/)
[session-replay-screenshots/](https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/).

26 ²⁵ *Id.*
27 ²⁶ Nitasha Tiku, *The Dark Side of ‘Replay Sessions’ That Record Your Every Move*
Online, WIRED (Nov. 16, 2017), [https://www.wired.com/story/the-dark-side-of-](https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/)
[replay-sessions-that-record-your-every-move-online/](https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/).

28 ²⁷ Englehardt, *supra* note 17.

²⁸ Tiku, *supra* note 25.

1 42. Recognizing the privacy concerns posed by Session Replay Code, in 2019
2 Apple required app developers to remove or properly disclose the use of analytics code
3 that allow app developers to record how a user interacts with their iPhone apps or face
4 immediate removal from the app store.²⁹ In announcing this decision, Apple stated:
5 “Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review
6 Guidelines require that apps request explicit user consent and provide a clear visual
7 indication when recording, logging, or otherwise making a record of user activity.”³⁰

8 **D. Spirit Secretly Wiretaps its Website Visitors’ Electronic**
9 **Communications.**

10 43. Spirit operates the website www.spirit.com. Spirit is a commercial airline
11 which provides both national and international flights to the public.

12 44. However, unbeknownst to the millions of individuals perusing Spirit’s
13 flights online, and booking (and paying for) Spirit airline tickets to and/or from
14 California airports, Spirit intentionally procures and embeds various Session Replay
15 Codes from Session Replay Providers on its website to track and analyze website user
16 interactions with www.spirit.com.

17 45. One such Session Replay Provider that Spirit procures is FullStory.

18 46. FullStory is the owner and operator of a Session Replay Code titled
19 FullStory Script, which records all website visitor actions, including information typed
20 by the website use while on the website. Such information can include names, emails,
21 phone numbers, addresses, social security numbers, date of birth, and more. Research
22 by the Princeton University Center for Information Technology Policy found that “text
23 typed into forms is collected before the user submits the form, and precise mouse
24 movements are saved, all without any visual indication to the user.”³¹

25
26 ²⁹ Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen*
Recording Code, TechCrunch (Feb. 7, 2019),
27 <https://techcrunch.com/2019/02/07/apple-glassbox-apps/>.

28 ³⁰ *Id.*
³¹ Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay*
scripts, Freedom to Tinker (Nov. 15, 2017), <https://freedom-to->

1 47. As a user interacts with any website with the embedded FullStory Script,
2 “each click, tap, URL visit, and every other interaction is sent in tiny little packets to
3 that existing session at FullStory servers.”³² This includes button clicks, mouse
4 movements, scrolling, resizing, touches (for mobile browsers), key presses, page
5 navigation, changes to visual elements in the browsers, network requests, and more.³³

6 48. Spirit’s procurement and use of FullStory’s Session Replay Code, and
7 procurement and use of other Session Replay Codes through various Session Replay
8 Providers, is a wiretap in violation California statutory and common law.

9 **E. Plaintiff’s and Class Members’ Experience.**

10 49. Plaintiff has visited www.spirit.com on her computer and/or smartphone
11 while in California to, *inter alia*, obtain information on flight pricing and to book (and
12 pay for) Spirit airline tickets. Plaintiff completed these transactions with Spirit within
13 the State of California.

14 50. While visiting Spirit’s website, Plaintiff fell victim to Defendant’s
15 unlawful monitoring, recording, and collection of Plaintiff’s Website Communications
16 with www.spirit.com.

17 51. Unknown to Plaintiff, Spirit procures and embeds Session Replay Code
18 on its website.

19 52. During the website visit, Plaintiff’s Website Communications were
20 captured by Session Replay Code and sent to various Session Replay Providers.

21 53. For example, when visiting www.spirit.com, if a website user searches for
22 a certain product, such as a specific flight, that information is captured by the Session
23 Replay Codes embedded on the website.

24
25 _____
26 tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

27 ³² *Id.*
28 ³³ *How does FullStory capture data to recreate my users’ experience?*, FullStory, <https://help.fullstory.com/hc/en-us/articles/360032975773-How-does-FullStory-capture-data-to-recreate-my-users-experience->, (last visited Nov. 7, 2022) (hereinafter “FullStory Data Capture”).

1 All natural persons in California whose Website Communications were
2 captured through the use of Session Replay Code embedded in
3 www.spirit.com

4 61. Excluded from the Class is Defendant, its parents, subsidiaries, affiliates,
5 officers, and directors, all persons who make a timely election to be excluded from the
6 Class, the judge to whom this case is assigned and any immediate family members
7 thereof, and the attorneys who enter their appearance in this action.

8 62. **Numerosity:** The members of the Class are so numerous that individual
9 joinder of all Class members is impracticable. The precise number of Class members
10 and their identities may be obtained from the books and records of Spirit or the Session
11 Replay Providers.

12 63. **Commonality:** This action involves questions of law and fact that are
13 common to the Class members. Such common questions include, but are not limited
14 to: (a) whether Defendant procures Session Replay Providers to intercept Spirit's
15 website visitors' Website Communications; (b) whether Spirit intentionally discloses
16 the intercepted Website Communications of its website users; (c) whether Defendant
17 acquires the contents of website users' Website Communications without their consent;
18 (d) whether Defendant's conduct violates the California Invasion of Privacy Act, Cal.
19 Penal Code §630 *et seq.* and/or whether that conduct constitutes a tortious invasion of
20 privacy and/or intrusion on seclusion; (e) whether Plaintiff and the Class members are
21 entitled to equitable relief; and (f) whether Plaintiff and the Class members are entitled
22 to actual, statutory, punitive, or other forms of damages, and other monetary relief.

23 64. **Typicality:** Plaintiff's claims are typical of the other Class members'
24 claims because, among other things, all Class members were comparably injured
25 through the uniform prohibited conduct described above. For instance, Plaintiff and
26 each member of the Class had their communications intercepted in violation of the law
27 and their right to privacy. This uniform injury and the legal theories that underpin
28 recovery make the claims of Plaintiff and the members of the Class typical of one
another.

1 **65. Adequacy of Representation:** Plaintiff has and will continue to fairly and
2 adequately represent and protect the interests of the Class. Plaintiff has retained counsel
3 competent and experienced in complex litigation and class actions, including litigations
4 to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests
5 of the Class, and Defendants have no defenses unique to Plaintiff. Plaintiff and her
6 counsel are committed to vigorously prosecuting this action on behalf of the members
7 of the Class, and they have the resources to do so. Neither Plaintiff nor her counsel
8 have any interest adverse to the interests of the other members of the Class.

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

16 **67. Predominance:** Common questions of law and fact predominate over any
17 questions affecting only individual Class members. Similar or identical violations,
18 business practices, and injuries are involved. Individual questions, if any, pale by
19 comparison, in both quality and quantity, to the numerous common questions that
20 dominate this action. For example, Defendants' liability and the fact of damages is
21 common to Plaintiff and each member of the Class. If Defendants intercepted
22 Plaintiff's and Class members' Website Communications, then Plaintiff and each Class
23 member suffered damages by that conduct.

24 **68. Ascertainability:** Members of the Class are ascertainable. Class
25 membership is defined using objective criteria and Class members may be readily
26 identified through Spirit' books and records or the Session Replay Providers' books
27 and records.

28

1 **COUNT I**

2 **VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT**

3 **Cal. Penal Code § 630 et. seq.**

4 69. Plaintiff incorporates the above allegations by reference as if fully set
5 forth herein and brings this count individually and on behalf of the Class.

6 70. The California Invasion of Privacy Act (“CIPA”) is codified at Cal. Penal
7 Code §§ 630-638. The Act contains the following statement of purpose:

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

14 71. California Penal Code § 631(a) accordingly provides, in pertinent part:

15 Any person who, by means of any machine, instrument, or contrivance, or
16 in any other manner . . . willfully and without the consent of all parties to
17 the communication, or in any unauthorized manner, reads, or attempts to
18 read, or to learn the contents or meaning of any message, report, or
19 communication while the same is in transit or passing over any wire, line,
20 or cable, or is being sent from, or received at any place within this state;
21 or who uses, or attempts to use, in any manner, or for any purpose, or to
22 communicate in any way, any information so obtained, or who aids, agrees
23 with, employs, or conspires with any person or persons to unlawfully do,
24 or permit, or cause to be done any of the acts or things mentioned above
25 in this section, is punishable by a fine not exceeding two thousand five
26 hundred dollars (\$2,500).

27 72. At all relevant times, Spirit’s business practice of injecting Session Replay
28 Code allowed it to access, intercept, learn the contents of and collect Plaintiff and Class
members’ personally identifiable information and other data.

73. Plaintiff, and each Class Member, visited and/or interacted with the Spirit
website while in California.

74. Plaintiff and Class members did not consent to any of Spirit’s actions in
intercepting, reading, and learning the contents of their communications

75. Spirit’s conduct was intentional in that it purposefully installed code
which allows it to eavesdrop and learn the content of its users’ communications and
other browsing activities that would otherwise be unavailable to Spirit without

1 engaging in this practice. Spirit directly participated in the interception, reading, and/or
2 learning of the contents of the communications between Plaintiff, Class members and
3 California-based web entities.

4 76. The information Spirit intercepts while Plaintiff and Class members are
5 using its website includes personally identifiable information and other highly specific
6 information and communications, including, without limitation, every button,
7 keystroke and link a user taps, whether the user has taken any screenshots, text entries
8 (including passwords and credit card information), and how much time a user spent on
9 the website.

10 77. Plaintiff and Class members have suffered loss by reason of these
11 violations, including but not limited to, violation of the right to privacy. Unless
12 restrained and enjoined, Spirit will continue to commit such acts.

13 78. As a result of the above violations and pursuant to CIPA section 637.2,
14 Spirit is liable to Plaintiff and Class members for the greater of treble actual damages
15 related to their loss of privacy in an amount to be determined at trial or for statutory
16 damages in the amount of \$5,000 per violation. Section 637.2 provides “[it] is not a
17 necessary prerequisite to an action pursuant to this section that the plaintiffs has
18 suffered, or be threatened with, actual damages.”

19 79. Plaintiff further requests, as provided under CIPA, reasonable attorneys’
20 fees and costs of suit, injunctive and declaratory relief, and punitive damages in an
21 amount to be determined by a jury sufficient to prevent or deter the same or similar
22 conduct by Spirit.

23 **COUNT II**

24 **INVASION OF PRIVACY – INTRUSION UPON SECLUSION**

25 80. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

26 81. California law recognizes the tort of invasion of privacy/intrusion on
27 seclusion.

28 82. Plaintiff brings this claim individually and on behalf of the Class.

1 83. Plaintiff and Class members have an objective, reasonable expectation of
2 privacy in their Website Communications.

3 84. Plaintiff and Class members did not consent to, authorize, or know about
4 Spirit's invasion/intrusion at the time it occurred. Plaintiff and Class members never
5 agreed that Spirit could collect or disclose their Website Communications.

6 85. Plaintiff and Class members had an objective interest in precluding the
7 dissemination and/or misuse of their information and communications and in
8 conducting their personal activities without intrusion or interference, including the
9 right to not have their personal information intercepted and utilized for business gain.

10 86. Spirit intentionally intrudes on Plaintiff's and Class members' private life,
11 seclusion, or solitude, without consent.

12 87. Spirit's conduct is highly objectionable to a reasonable person and
13 constitutes an egregious breach of the social norms underlying the right to privacy.

14 88. Plaintiff and Class members were harmed by Spirit's wrongful conduct as
15 Spirit's conduct has caused Plaintiff and the Class mental anguish and suffering arising
16 from their loss of privacy and confidentiality of their electronic communications.

17 89. Spirit's conduct has needlessly harmed Plaintiff and the Class by
18 capturing intimately personal facts and data in the form of their Website
19 Communications. This disclosure and loss of privacy and confidentiality has caused
20 Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear,
21 and other harms.

22 90. Additionally, given the monetary value of individual personal
23 information, Defendant deprived Plaintiff and Class members of the economic value
24 of their interactions with Defendant's website, without providing proper consideration
25 for Plaintiff's and Class members' property.

26 91. Further, Spirit has improperly profited from its invasion of Plaintiff and
27 Class members' privacy in its use of their data for its economic value.

28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

DATED: February 7, 2023

Respectfully Submitted

/s/Steven M. Nathan
Steven M. Nathan, SBN 153250
HAUSFELD LLP
33 Whitehall Street
Fourteenth Floor
New York, NY 10004
Telephone: (646) 357-1100
Email: snathan@hausfeld.com

James J. Pizzirusso, D.C. Bar No.
477604
HAUSFELD LLP
888 16th Street N.W.
Suite 300
Washington, D.C. 20006
Telephone: (202) 540-7200
Email: jpizzirusso@hausfeld.com

Stephen B. Murray, La. Bar No. 9858
Stephen B. Murray, Jr, La. Bar No.
23877
Arthur M. Murray, La. Bar No. 27694
Thomas M. Beh, La. Bar No. 24018
THE MURRAY LAW FIRM
701 Poydras Street, Suite 4250
New Orleans, Louisiana 70139
Telephone: (504) 525-8100
Email: Tbeh@Murray-lawfirm.com
Attorneys for Plaintiff

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Accuses Spirit Airlines of Tracking Website Visitors Without Consent](#)
