UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

ANDREW PHILLIPS, on behalf of himself and all others similarly situated,

Plaintiff,

v.

JETBLUE AIRWAYS CORPORATION,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff ANDREW PHILLIPS ("Plaintiff") brings this class action complaint (the "Action") on behalf of himself and others similarly situated for violations of federal, state, and common law against Defendant, JETBLUE AIRWAYS CORPORATION ("JetBlue" or the "Defendant") upon personal knowledge as to himself and his own actions, information and belief, and the investigation of his counsel, seeking actual damages, statutory damages, restitution, disgorgement of profits into a constructive trust, pre- and post-judgment interest, reasonable costs and attorneys' fees, a declaratory judgment, injunctive relief, and any other relief this Court deems just and proper, as follows:

INTRODUCTION

1. This is one of the very first class actions in American history regarding dynamic surveillance pricing and the surreptitious use of consumer data in order to set pricing based on consumer behavior.

2. Plaintiff and Class members are airline travelers who have used Defendant's website, *www.jetblue.com*, within the statutory period to book airline travel and acquire airline tickets on JetBlue's airlines as well as the airlines which codeshare with JetBlue.

3. Defendant offers services related to airline travel.

4. The data associated with air travel is highly sensitive because it involves the collection of personally identifiable information as well as the specific transaction data related to Plaintiff's air travel.

5. For example, if a user of Defendant's website is seeking airline tickets for travel purposes the website must combine identifiers (*e.g.* the travelers' name, connected accounts including their email address, and their internet protocol address) together with other information including the data needed to book airfare (government identification, full name, address and other information) as well as information about the airfare itself (travel information) and payment information.[1]

6. The digital booking of Defendant's airfare services come with a reasonable expectation of privacy because of the sensitive nature of the PII provided, and thus Defendant's website users have the very same privacy rights as those who physically walk up to an airline ticketing counter. With that in mind, ordinarily, a traveler would have to consent to the presence of other third-parties looking over their shoulders or

[1] Taken together with personally identifiable information such as a customer identifier, internet protocol address, or other information which identifies a specific person, the "PII."

being at an airline ticketing counter along with them as they transact business with and provide PII to an airline, as is the case here.

7. However, rather than protect their PII, Defendant uses tracking technology itself and otherwise allows third parties, to collect, retain, and use traveler data without adequate and sufficient consent from Plaintiff and Class members using tracking technology embedded in website code. The existence of the trackers used by Defendant and by third parties on the website is a breach of travelers' privacy.

8. This is especially so considering the methodology and purpose for deploying these technologies are not adequately disclosed: while Defendant has a Privacy Policy, it: (1) does not disclose that the trackers are used to set pricing (*e.g.* when a consumer searches for airline tickets and then closes the browser window, the prices increase when the consumer seeks to re-engage with purchasing), (2) it does not disclose that the trackers are used for behavioral analytics which also allow the airline to set pricing dynamically as opposed to set, static pricing, and (3) it generally does not disclose that it shares consumer data with third parties for the purpose of setting prices.

9. However, JetBlue shares consumer data with numerous third parties. In fact, Defendant admitted on social media that they use this form of dynamic surveillance pricing, as can be seen below on April 18, 2026:

10. Sharing information with third parties and allowing them to secretly collect this information makes this possible.

11. For example, FullStory, Inc., a behavioral analytics and data collection platform which provides Fullstory's "behavior data platform to optimize its digital experience [b]y closely monitoring revenue-impacting features and enhancing user flows" services using data collection, behavioral analysis, and user targeting, uses trackers to

collect data on numerous pages on Defendant's website.[2] According to JetBlue's Digital Experience Product Manager, Greg Kaplan, "[w]ith FullStory, we can make product decisions faster. If an issue crops up, I can see how big its impact is within two minutes and determine how we should prioritize it. With other tools, there can be a significant lead time between when the data is logged and when it's indexed and available – it's been so valuable to have the data at our fingertips immediately."[3]

12. Additionally, JetBlue shares consumer data with a company called PROS Holdings, Inc., which uses an algorithm to set pricing in real time based on "buyer behavior" as discussed more below.

13. Naturally, Defendant deleted their social media post and denied that dynamic surveillance pricing takes place – but the website code, other public statements, and this admission on social media all say otherwise. And while setting higher prices based on consumer behavior is abhorrent – this Action is focused on the violations of consumer

[2] https://www.fullstory.com/customer-story/travel-hospitality/jetblue/?utm_source=google&utm_medium=paid-search&utm_campaign=GS-2024-Demo-Brand&utm_offer=demo&utm_product=AN&utm_term=fullstory&gad_source=1&gad_campaignid=21245150379&gbraid=0AAAADmJjBSlgmSQDc1P7B5VkyxmrcdkT&gclid=EAIaIQobChMIy7_Fnv2BlAMV-WlHAR0BTSzbEAAYASAAEgK9R_D_BwE, (last accessed Apr. 22, 2026).

[3] *Id.*

privacy who book flights on Defendant's website. Consumers should not have to have their privacy rights violated to participate in Defendant's digital rat race for airline tickets which should cost the same for each similarly seated passenger.

14. Dynamic surveillance pricing, and, specifically, JetBlue's conduct from this past week, has drawn consternation from Congress and federal regulatory authorities.

15. As such, Defendant has blatantly invaded or allowed for the invasion of Plaintiff and Class members' privacy rights. Plaintiff seeks to rectify these harms under federal, state, and common law causes of action, pursuing actual damages, statutory damages, pre- and post-judgment interest, reasonable costs and attorneys' fees, a declaratory judgment, injunctive relief and any other relief this Court deems just and proper.

JURISDICTION AND VENUE

16. *Subject Matter Jurisdiction.* This Court has federal question subject matter jurisdiction pursuant to 28 U.S.C. § 1331 as well as pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). As required by CAFA, 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 Defendant. Namely, numerous members of the putative Class are domiciled in states around the country other than New York.

17. Additionally, this Court has supplemental jurisdiction over Plaintiff's state law claims which are anchored by Plaintiff's Electronic Communications Privacy Act claim.

18. *Personal Jurisdiction.* This Court has personal jurisdiction over the litigants because Plaintiff Phillips is located in New York, Defendant is headquartered in New York, Defendant is registered to do business in New York, Defendant's acts or practices were directed toward this State (and thus, Defendant intentionally availed itself of this jurisdiction by choosing to do business in New York) and, since the Defendant website is used throughout the United States, Defendant knew or should have known that tracking technologies were being used to intercept the actions of Class members in New York.

19. *Venue.* Venue is proper because Defendant is headquartered in and conducts business in this District, (2) Defendant's acts or

omissions were directed toward this District, (3) a substantial part of the events, acts and omissions giving rise to Class members' claims occurred here, and (4) because Class members were harmed here.

PARTIES

PLAINTIFF

Plaintiff Andrew Phillips

20. Plaintiff Phillips is domiciled in the state of New York.

21. During the relevant period, in December of 2025, Plaintiff Phillips visited Defendant's website to book airfare on Defendant's website, including a flight from New York to Florida. Plaintiff Phillips provided his destination and arrival locations, information on his desired form of airfare accommodations *(e.g.,* his seating), the personally identifiable information required to book a flight (*e.g.*, his name, address, government identification numbers, gender, etc.) and his payment information. Additionally, the tracking code collects other information, including whether or not the Plaintiff closed the website, a Google identifier, and other data which is detailed below.

22. While on Defendant's website, Plaintiff Phillips was entirely unaware that he was being tracked for the purpose of setting pricing.

23. Not only was Plaintiff Phillips not adequately informed about the sale of his data to these third parties, but he was not adequately given compensation for his sensitive and valuable information.

24. Plaintiff Phillips has suffered the following injuries from (1) the interception of his private and valuable data, (2) the disclosure of his private and valuable data to unauthorized third parties, and (3) the failure to justly compensate Plaintiff Phillips for his valuable information:

a. The loss of value of personally identifiable information and/or travel data that might be associated with Plaintiff Phillips' visits to Defendant's website;

b. Intrusion upon Plaintiff Phillips' and Class members' privacy on Defendant's website where it was reasonable for Plaintiff Phillips and Class members to have an expectation of privacy;

c. Lack of compensation for the sale of Plaintiff Phillips and Class members' data; and

d. Profiting from the collection, retention, use and/or sale of Plaintiff Phillips and Class members' data in a way that would be inequitable sans disgorgement of profit.

25. Had Plaintiff Phillips known about the surreptitious collection and tracking of his PII, he would not have used a different airline or booked travel a third party travel website.

DEFENDANT

Defendant JetBlue Airways Corporation

26. Defendant JetBlue Airways Corporation is a corporation with its principal place of business located in Long Island City, New York.

27. Defendant is a sophisticated business that provides airline tickets and other airfare to millions of Americans on an annual basis – indeed, it is one of the largest airlines in the United States.

28. In the course of doing business, Defendant maintains a website at the following URL address: *www.jetblue.com*. This website is used by patients seeking airline tickets, like Plaintiff and Class members.

FACTUAL ALLEGATIONS

Defendant's Business and Data Collection

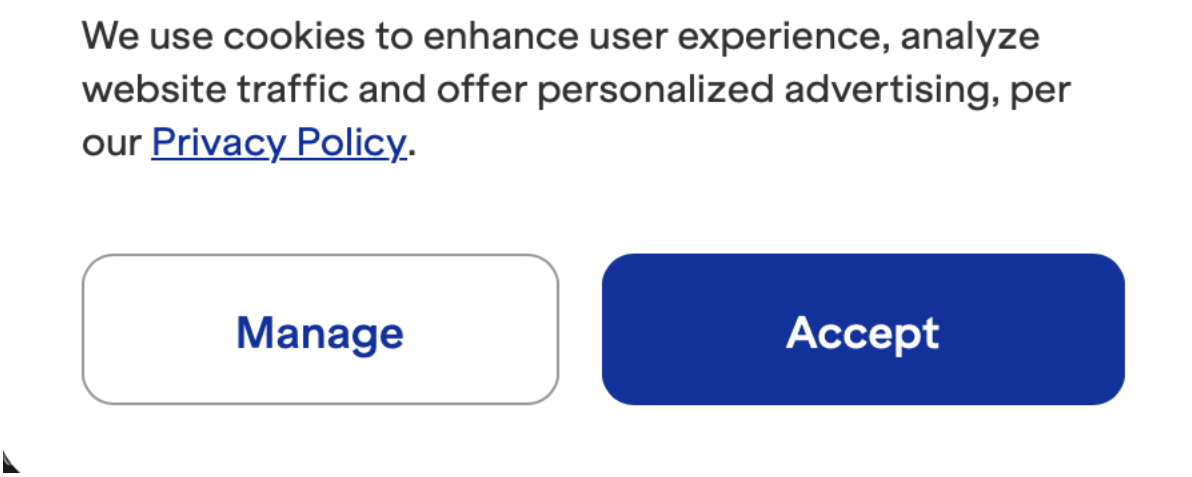
29. Defendant is an American low-cost airline which is headquartered in Queens, New York City. Defendant's primary hub is John F. Kennedy International Airport, which destinations across the United States. Currently, Defendant has over 279 planes in their fleet and travels to 111 destinations.

30. Defendant provides flights to airline fliers by assisting with the process of booking both through its website and on third party websites. In order to do this, the patients who use the Defendant's website provide Defendant with significant data to find the right flight(s).

31. By its very nature, Defendant – a business which is frequented by Plaintiff and Class members – is the type of business that requires heightened levels of privacy. The collection of data is highly sensitive, which is why Defendant promises discretion both in the way

it conducts its business as well as with respect to the data it collects through its website (and through other means). Including in its "privacy choices" page which states that "[o]ur privacy commitments are fundamental to the way we run our business" and that "[Defendant] may share information that does not identify you (including information that has been aggregated or de-identified)." This can be seen below:

32. Additionally, the banner pop-up which Defendant uses does not disclose the use of data collection for the purpose of surveillance pricing:



33. No reasonable consumer would presume that this banner pop-up would include the collection and use of their data through cookies to set pricing – let alone to share it with third parties to do so.

34. Furthermore, Defendant initially seems to understand the critical nature of protecting passenger data; but immediately contradicts itself stating that aspects of the website do not work unless users opt into the data sharing. Even so – if consumers opt into Defendant's data sharing, the Privacy Policy does not disclose that their information is being used to set prices. In fact, these are the only purposes for data collection, retention, and use that Defendant discloses with respect to its Privacy Policy:

a. Use by Service Providers (payment processing, travel and booking reservation, identity verification, data analytics,

marketing and advertising, website hosting, and technical support);

b. Vendors and Other Parties (advertising and analytics);

c. Affiliates (customer support, marketing, booking, advertising and technical operations);

d. Partners (for services and distribution of products or joint ventures);

e. Promotions;

f. Public Forums;

g. Merger and Acquisition;

h. Security or Compelled Disclosure (to law enforcement and other authorities);

i. Facilitating Requests (via social media); and

j. Consent.

35. There are no disclosures of the use of consumer data for the purpose of dynamic surveillance pricing. And the data that the Privacy Policy purports to collect is vast:

a. Contact Data (first and last name, email address, postal address, telephone number);

b. Billing Information;

c. Demographic Data (age, gender, and country of origin);

d. Profile Data (interests, inferences, preferences, and favorites);

e. Content (posted on forums or on JetBlue's blogs);

f. Personal Contacts and Passenger Data;

g. Job Applicant Data (if applicable);

36. Finally, Defendant lists the types of data collected through tracking technology (while not disclosing that the end use is for dynamic surveillance pricing):

a. Internet Protocol address;

b. Device Identifier;

c. Browser Type and Version;

d. Operating System and Platform;

e. Mobile Device Type;

f. Wireless Carrier;

g. Data Regarding Network Connected Hardware;

h. The Time Spent Engaging With JetBlue's Services;

i. Page Views;

j. Information Searched For;

k. Geo-Location Data;

l. Pages Visited;

m. Content and Advertisements Viewed;

n. Products and Services Viewed;

o. Purchases and Purchase History;

p. Time of Day When Browsing;

q. Referring Pages; and,

r. Exiting Pages.

37. Defendant makes privacy assurances and representations which directly contradict the reason and rationale for the types of data that they collect. Privacy-based representations are material components of the services that Defendant has to offer through its website: Defendant knows this otherwise those representations (which, as discussed below, are false) and the manner in which those representations are made are done so to drive goodwill, website traffic, and consumer trust to Defendant.

38. Defendant can also make significant assumptions based off of the data it collects which impact pricing. For example, historically,

the "Operating System and Platform" a consumer uses may seem benign – but it is commonly weaponized as a means to tell the socioeconomic status of a consumer, as those who use Apple's iOS operating system and platforms are often wealthier than those who use an Android operating system and platform. Additionally, Defendant collects information about the geographic location (geo-location) of consumers, which allows them to adjust prices based on someone's zip code or the socioeconomic class of where they live or are located.

39. This is all highly concerning. It allows Defendant to manipulate prices in real time in order to make as much money as they can on fares for airline tickets which are priced differently for consumers based on their private information which they did not consent to surrender for this purpose.

Defendant's Surveillance Pricing

40. Rather than keep this private information (the information collected as well as the datapoint itself that Plaintiff had visited the JetBlue website at all) protected, Defendant instead opted to make it available for collection, weaponize it for pricing purposes, and share it with other third parties like FullStory and PROS.

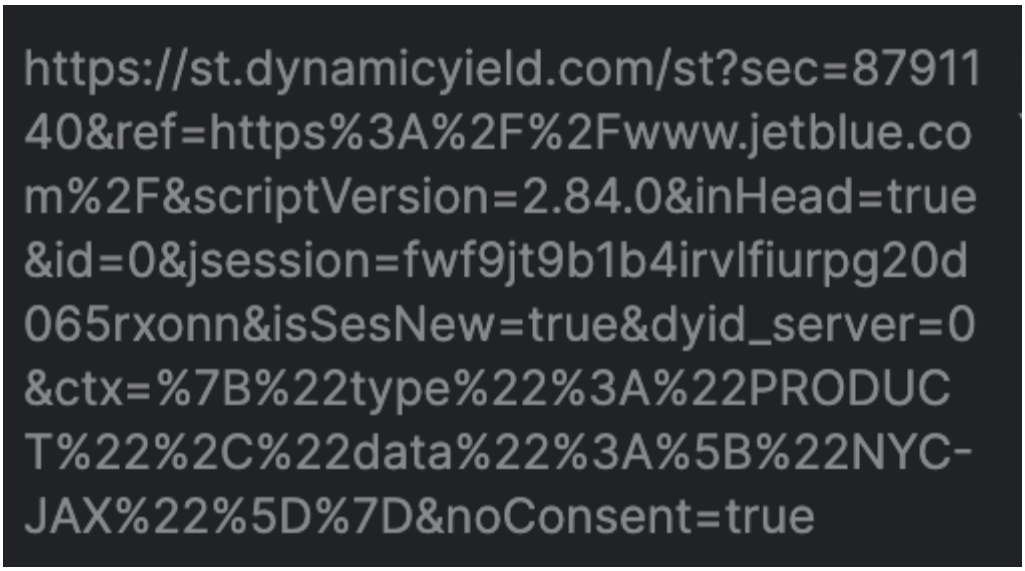
41. Defendant either knew (and was likely profiting from) or should have known that third parties were using its website to collect data. It defies logic to believe that FullStory and PROS would merely collect, retain, and otherwise use Defendant's data for free. These third parties used tracking technologies to collect data on Plaintiff and Class members, then used those technologies to analyze consumer behavior and ultimately change prices.

42. For example, this line of code shows the presence of FullStory on JetBlue's homepage where consumers can enter in information seeking flights. It shows that FullStory has tracking technology on this page, and the use of the code in its URL address, "^$3p" denotes a request for data from a third party.

43. Other third parties are present on JetBlue's homepage, including other analytics firms such as TrustArc, which collects

information including when a page is open or closed as well as when a new session is started on JetBlue's website:

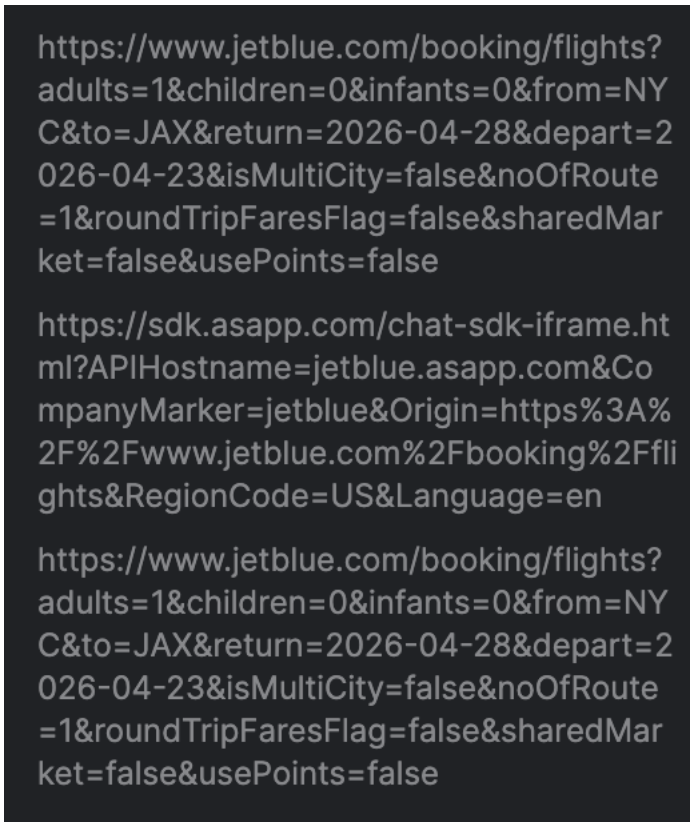
44. Counsel for Plaintiff Phillips then replicated the same search for a flight from New York to Jacksonville, to find additional tracking mechanisms:



45. JetBlue also allows for the presence of Google Tag Pixels, which individually identify consumers, contrary to the privacy policy's promise to otherwise not do so.

46. JetBlue itself uses tracking mechanisms through cookies which can be used to set pricing. For example, JetBlue collects a

substantial amount of consumer data using tracking technologies when booking the same flight which Plaintiff Phillips had booked in December of 2025:



47. As seen in the code, it collects the passenger type (adults, children or infants), the departure and destination data, the proposed dates of travel, whether or not the fares should be flagged as round trip (which presumably impacts the price) the booking origin (Defendant's website), the region of booking (United States) and the language used to book the flight (English). Each of these are data points which do not need to be collected through surreptitious tracking technology –

especially given that a consumer would willingly give them over to the Defendant. The reason for this is because this data is necessary to feed into algorithms from JetBlue directly to third parties like PROS.

48. JetBlue uses dynamic pricing powered by its own data since 2024.[4] Apparently, airlines have used dynamic pricing for decades – including products like those created by PROS – which JetBlue currently uses. In fact, when JetBlue began to use PROS revenue management dynamic pricing system, PROS touted its use as a "customer success story." At the time, on June 13, 2025, PROS stated, "JetBlue set out to solve a persistent challenge: forecast accuracy. With previous revenue management systems falling short, the team was forced to rely heavily on manual overrides – hindering efficiency and trust in the data."

49. The job of PROS is to set prices through algorithms, and algorithms due this through the collection of data. According to the Financial Times in 2017, "PROS says its algorithms set more prices each day than Twitter sends tweets."

50. Today, PROS uses real-time dynamic pricing which sets pricing at the time of the transaction to maximize revenue – the only

[4] https://www.timeout.com/usa/news/jetblue-increased-its-bag-fees-as-oil-prices-rise-033126, (last accessed April 22, 2026).

way that PROS would be able to set said pricing is to have the data points to do it: which come from consumers. As PROS explains, its real time dynamic pricing "enables airlines to offer prices to their customers based on contextual information available at the time of shopping." PROS has a model of this on its website:

Continuous Pricing

PROS Real-Time Dynamic Pricing supports AI-driven continuous pricing, helping airlines offer fares between predefined price levels instead of relying on rigid class-based pricing. This scientific approach uses real-time data and advanced algorithms to adjust fares dynamically, capturing hidden demand and increasing revenue with more precise, market-responsive pricing.

51. Additionally, PROS's 2024 annual report states that their software adapts based on the particular customer, "[o]ur AI-powered

algorithms provide market relevant price guidance, dynamically refining prices in response to changing market conditions and buyer behavior. This predictive and prescriptive price guidance tailors pricing for each unique buying scenario."

52. Again, none of this would have been possible had JetBlue not been collecting this data in the first instance: let alone sharing it with third parties like FullStory, PROS and others.

53. However, the picture becomes clearer considering JetBlue itself admitted to using cookie collected data on its booking pages in order to adjust airfare pricing. Which, again, can be seen below:

54. This sensitive information and identifying data is highly valuable, and because a variety of different end-users could have

utilization for it, it maintains its value as it is collected, sold, and resold. Defendant allows for the collection of this data at its primary source: directly from Plaintiff and Class members themselves.

55. The reason that Defendant collects this data is because it has an even higher value than ordinary data – it allows tangible increases in pricing for airline tickets, which Defendant admitted.

The Harms of Surveillance Pricing

56. Surveillance pricing is the use of personal data, like "browsing history, spending habits, location, or even signals about […] income to figure out what you're likely willing to pay and then adjust accordingly."[5] While surveillance pricing is not illegal in the United States, secretly collecting consumer data on the internet without adequate consent is - and that is the basis for this Action.

57. According to Lindsay Owens, a privacy expert who leads the Groundwork Collaborative think-tank: "JetBlue accidentally tweeted their cold-blooded confession that they are using consumers' search history against them to drive up prices."[6]

[5] https://www.travelpirates.com/captains-log/jetblue-surveillance-pricing-explained, (last accessed Apr. 22, 2026).

[6] *Id.*

58. According to Grace Gedye, senior policy analyst at Consumer Reports: "We are seeing more evidence of these types of pricing practices and call on lawmakers to introduce new rules that would require transparency in pricing practices and prohibit surveillance pricing."[7]

59. Naturally, JetBlue denied this practice, stating that the admission was "incorrect and we apologize for the error." It also added "JetBlue fares on JetBlue.com and our mobile app[lication] are not determined by cached data or any other personal information. We do not use AI or personal data to set individual pricing. All customers have access to the same fares."[8]

60. The Federal Trade Commission ("FTC") has begun to define the mechanics of surveillance pricing:

[7] *Id.*
[8] *Id.*

61. According to former FTC Commissioner Lina M. Khan, "Firms that harvest Americans' personal data can put people's privacy at risk. Now firms could be exploiting this vast trove of personal information to charge people higher prices. Americans deserve to know

whether businesses are using detailed consumer data to deploy surveillance pricing."[9]

62. Additionally, Congress is now taking action against JetBlue for their use of surveillance pricing, including a letter sent by United States Senator Ruben Gallego and House of Representatives member Greg Casar which called for responses to JetBlue's use of personal data for setting of fare prices.[10] In part the letter states about the social media post, "[w]hile JetBlue claimed in the wake of this post that fares are not 'determined' by cached data or personal information, this exchange raises questions about how JetBlue sets prices – specifically, how JetBlue is defining personal data and whether the personal data is used in any capacity to inform prices. We are especially concerned that customers could be charged different prices for the same flight based on their need for travel, such as attending a funeral."[11]

63. Defendant's conduct violates numerous laws as well as basic notions of consumer privacy.

---

[9] https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-issues-orders-eight-companies-seeking-information-surveillance-pricing, (last accessed Apr. 22, 2026).

[10] **Exhibit A**: Letter from Congress to JetBlue Airlines re Surveillance Pricing.

[11] *Id.*

Defendant's Conduct Offends Basic Privacy Rights.

64. Defendant's services come with a reasonable expectation of privacy that exists because of the sensitive nature of the type of work that Defendant does and the representations that Defendant makes on its website. The same holds true for airline passengers who electronically walk into digital storefronts. These airline passengers deserve the same privacy rights afforded to ordinary consumers who walk up to a physical ticketing counter. This is especially true here, where Plaintiff and Class members did not anticipate, invite, or adequately consent to the presence of other third-party corporations looking over their digital shoulders as they transact business with Defendant.

65. The identifying datapoints collected by Defendant (device identifiers, internet protocol address(es), usernames and login information, etc.) in tandem with the information that Plaintiff accessed Defendant's website to procure services, on their own, is highly sensitive information.

66. Rather than protect this information, as well as other potential data collected Defendant allows it to be collected, retained and

used by third parties which lack sufficient consent from Plaintiff and Class members to do so.

The Value of Consumer Data

67. Plaintiff and Class members were harmed when Defendant invaded their privacy rights by weaponizing their data for surveillance pricing through Defendant's website. Reasonable airline passengers, who are consumers, would not have used Defendant's website had they known that their privacy rights would be invaded as a result.

68. PII is extremely valuable. There is a huge market for the data collected on Defendant's website. Plaintiff and Class members have suffered pecuniary losses when Defendant sold and allowed for the resale of their data to unauthorized third parties because of the value of the data itself. The market for this data also has tangible value – including the use of the data to increase prices for airfare tickets.

Harm to Consumers

69. Plaintiff and Class members provided their data to Defendant to obtain information regarding the travel services that Defendant provides – services which happen to be highly personal and

very private. This information was disclosed to and intercepted by the third-parties, including FullStory, as listed herein through digital tracking technology. This information was collected and intercepted for business purposes, including to monitor consumer behavior and adjust airline pricing accordingly.

70. Plaintiff did not adequately consent to the interception or disclosure of their data to these third parties, or to anyone else. As such, Plaintiff have suffered from the type of privacy-centric harms that a patchwork of privacy protections which federal, state, and common law principles were intended to collectively protect against.

CLASS ACTION ALLEGATIONS

71. Plaintiff brings this Action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Classes (collectively, the "Class"):

> **Nationwide Class:** All natural persons in the United States who used the Defendant's website and/or mobile application and whose communications and/or data was shared with third parties during the applicable statutory period.
>
> **New York Sub-Class:** All natural persons in the state of New York who used the Defendant's website and/or mobile application and whose communications and/or data was shared with third parties during the applicable statutory

period.

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

73. ***Numerosity***. The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists of thousands or even millions of individuals, and the members can be identified through Defendant's records.

74. ***Predominant Common Questions***. 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:

a. Whether Defendant violated Plaintiff's and Class members'

privacy rights;

b. Whether Defendant violated the Electronic Communications Privacy Act;

c. Whether Defendant's acts and practices violated state consumer protection laws;

d. Whether Defendant's conduct is a breach of implied contract;

e. Whether Defendant was unjustly enriched;

f. Whether Plaintiff and the Class are entitled to equitable relief, including but not limited to injunctive relief, restitution, and disgorgement; and,

g. Whether Plaintiff and the Class are entitled to actual, statutory, punitive and/or other forms of damages, and other monetary relief.

75. ***Typicality***. Plaintiff's claims are typical of the claims of the other members of the Class and arise from the same conduct by Defendant and are based on the same legal theories.

76. ***Adequate Representation***. Plaintiff have and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff have retained counsel competent and experienced in complex

litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to any victim. Plaintiff 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 Plaintiff nor their counsel have any interest adverse to the interests of the other members of the Class.

77. 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.

78. Plaintiff may revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

FIRST CAUSE OF ACTION

VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2510 *et seq.*
(ON BEHALF OF THE NATIONWIDE CLASS)

79. Plaintiff re-alleges and incorporates all preceding paragraphs with the same force and effect as if fully restated herein.

80. The Electronic Communications Privacy Act ("ECPA") makes it illegal intentionally to intercept, or attempt to intercept, any wire, oral, or electronic communication and to disclose or use the contents of an unlawfully intercepted communication. 18 U.S.C. § 2511.

81. ECPA provides a private right of action to any person whose electronic communications are intercepted. 18 U.S.C. § 2520(a).

82. Defendant intentionally intercepted electronic communications that Plaintiff and the Class members exchanged with Defendant through the tracking tools installed on its website.

83. The transmission of data between Plaintiff and the Class members and Defendant qualify as communications under ECPA. 18 U.S.C. § 2510(12).

84. Defendant contemporaneously intercepted and transmitted

Plaintiff's and the Class members' communications of that data to the companies whose trackers Defendant installed or allowed to be installed on its website as well as for the purpose of engaging in third party tracking for behavioral analysis to modify ticket pricing.

85. The trackers that Defendant uses to track Plaintiff and the Class members' communications, Plaintiff and the Class members' browsers, Plaintiff and the Class members' computing devices, and the code that Defendant placed or allowed to be placed on its website are all "devices" within the meaning of 18 U.S.C. § 2510(5).

86. The third party companies, including FullStory, that are the recipients of communications between Plaintiff and the Class members, on the one hand, and Defendant, on the other, are not party to those communications.

87. Defendant transmits the contents of those communications through the surreptitious redirection of the communications from Plaintiff and the Class members' computing devices.

88. Plaintiff and the Class members did not consent to the third party companies' acquisition of their communications with Defendant. Nor did the third party companies receive adequate legal authorization

to receive such communications.

89. In disclosing the content of Plaintiff's and the Class members' communications relating to the purchase and use of Defendant's products, Defendant had a purpose that was tortious, criminal, and designed to violate statutory provisions including:

a. The unauthorized disclosure of individually identifiable information is tortious in and of itself, regardless whether the means deployed to disclose the information violates the ECPA or any subsequent purpose or use. Defendant intentionally committed a tortious act by disclosing individually personally identifiable information without authorization to do so;

b. Intrusion upon Plaintiff's and the Class members' seclusion;

c. Trespass upon Plaintiff's and the Class members' personal and private property; and

d. Violation of 18 U.S.C. §§ 1343 (fraud by wire, radio, or television) and 1349 (attempt and conspiracy) which prohibit a person from "devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by

> means of false or fraudulent pretenses, representations or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate … commerce, any writing, signs, signals, pictures, or sounds for purpose of executing such scheme or artifice."

90. The federal wire fraud statute, 18 U.S.C. § 1343, has four elements: (1) that the defendant voluntarily and intentionally devised a scheme to defraud another out of money or property; (2) that the defendant did so with intent to defraud; (3) that it was reasonably foreseeable that interstate wire communications would be used; and (4) that interstate wire communications were used. The attempt version of the statute provides that penalties apply to attempts as well as offenses. 18 U.S.C. § 1349.

91. Defendant's scheme or artifice to defraud consists of the false and misleading statements in its privacy policy described herein.

92. Defendant acted with intent to defraud in that it willfully invaded and took Plaintiff and the Class members' property, including the property rights to their individually personally identifiable information and their right to determine whether such information

remains confidential; the right to determine who may collect and use such information for marketing; and the right to determine who has access to their devices and communications.

93. Defendant also acted with intent to defraud in that it willfully invaded and took Plaintiff and the Class members' property (their PII) with knowledge that it lacked consent or authorization to do so; a reasonable consumer would not understand that Defendant was collecting and transmitting their data to third parties; a reasonable consumer would be shocked to realize the extent of Defendant's disclosure of data to third parties for the purpose of behavioral analytics and surveillance pricing

94. Defendant acted with the intent to acquire, use, and disclose Plaintiff's and the Class members' PII without their authorization or consent.

95. Plaintiff and the Class members have suffered damages because of Defendant's violations of ECPA, including that (1) Defendant eroded the essential, confidential nature of the relationship between Defendant and Class members, (2) Defendant derived valuable benefits from using and sharing Plaintiff and the Class members'

communications without their knowledge or informed consent and without providing compensation, (3) Defendant's actions deprived Plaintiff and the Class members of the value of their PII, (4) Defendant's actions diminished the value of Plaintiff's and the Class members' property rights in their PII; and (6) Defendant violated Plaintiff and the Class members' privacy rights by sharing their PII for commercial use.

96. Plaintiff and the Class members seek appropriate declaratory or equitable relief including injunctive relief, actual damages and profits enjoyed by Defendant due to the violations or the appropriate statutory measure of damages, punitive damages, and reasonable attorneys' fees and costs. 18 U.S.C. § 2520. Pursuant to 18 U.S.C. § 2520, Plaintiff and the Class members seek monetary damages for the greater of (i) the sum of the actual damages suffered by the plaintiff and any profits made by Defendant due to the violation or (ii) statutory damages of whichever is greater of $100 a day for each violation or $10,000.

97. Unless enjoined, Defendant will continue to commit the violations of law described herein.

SECOND CAUSE OF ACTION

VIOLATIONS OF NEW YORK'S DECEPTIVE TRADE PRACTICES ACT N.Y. GEN. BUS. LAW §349

(ON BEHALF OF BOTH THE NATIONWIDE CLASS AND STATE SUBCLASS)

98. Plaintiff re-alleges and incorporates all preceding paragraphs with the same force and effect as if fully restated herein.

99. Defendant is considered a 'business' under New York General Business Law 349 ("GBL 349").

100. Defendant's business acts and practices are unfair and deceptive under GBL 349. New York (as well as other states through their respective unfair and deceptive trade practices statutes) has a strong public policy of protecting consumers' privacy interests, including protecting consumers' personal data. Defendant violated GBL 349 by, among other things, disclosing and intercepting Plaintiff's and Class members' sensitive data, including private information, without consent.

101. Defendant further engaged in unfair business practices because it made material misrepresentations and omissions concerning the information that it assured users it would not share with third parties in the manner that it did, which deceived and misled users of Defendant's

platform.

102. Defendant's business acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm of Defendant secretly disclosing, intercepting, and misusing Plaintiff and Class members' sensitive and highly valuable personal data is significant, and there is no corresponding benefit resulting from such conduct.

103. Finally, because Plaintiff and Class members were completely unaware of Defendant's conduct, they could not have possibly avoided the harm.

104. Indeed, although Defendant's privacy policy states that Defendant uses and shares personal information in certain circumstances, Plaintiff and the Class members cannot give informed consent for this type of collection given it was not included in the privacy policy.

105. By unlawfully disclosing and intercepting this data, Defendant has taken money or property from Plaintiff and Class members.

106. Plaintiff and the Class Members seek all available damages under applicable state consumer protection laws, including statutory damages under GBL 349.

THIRD CAUSE OF ACTION

VIOLATIONS OF NEW YORK'S UNLAWFUL SELLING PRACTICES ACT N.Y. GEN. BUS. LAW §396

(ON BEHALF OF BOTH THE NATIONWIDE CLASS AND STATE SUBCLASSES)

107. Plaintiff re-alleges and incorporates all preceding paragraphs with the same force and effect as if fully restated herein.

108. Under New York General Business Law §396 (GBL §396), unlawful selling practices are prohibited and can be enforced by private plaintiffs in civil litigation.

109. Specifically, GBL §396 prohibits the offering "for sale any merchandise, commodity, or service, as part of a plan or scheme with the intent, design, or purpose not to sell the merchandise, commodity, or service so advertised at the price stated therein." GBL §396(1).

110. In this instance, Defendant sells the same airline tickets for set prices – only to change those prices with the intent not to sell them if the consumer's personal data determines otherwise. For example, if the

consumer, like Plaintiff Phillips, exits the Defendant's website, the Defendant then has the capacity to change prices and not sell them as advertised with the intent, design, or purpose to do so based on the personal information collected about Plaintiff Phillips.

111. Under this provision, Plaintiff and Class members can pursue actual damages, $500 per violation, attorneys' fees, and any other relief this Court deems just and proper.

DEMAND FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the proposed Class respectfully requests that the Court enter an order:

A. Certifying the Class and appointing Plaintiff as the Class representative;

B. Finding that Defendant's conduct was unlawful, as alleged herein;

C. Awarding declaratory relief against Defendant;

D. Awarding such injunctive and other equitable relief as the Court deems just and proper, including injunctive relief;

E. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages;

F. Awarding Plaintiff and the Class members pre-judgment and post-

judgment interest;

G. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

H. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

112. Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff demands a jury trial as to all issues triable by a jury.

DATED: April 22, 2026

Respectfully Submitted,

/s/ *Blake Hunter Yagman*
Blake Hunter Yagman
blake.yagman@yagmanpllc.com
YAGMAN PLLC
The Foundry Building
1050 30th Street, N.W.
Georgetown, Washington D.C. 20007
Telephone: 929-709-1493

Attorney for Plaintiff Phillips and the Proposed Classes