

BRETT A. SHUMATE
Assistant Attorney General, Civil Division
CODY M. POPLIN
Deputy Assistant Attorney General
HILARY K. PERKINS
Director
LISA K. HSIAO
Deputy Director
MARCUS P. SMITH
Assistant Director
AUSTIN T. MENDES
MEREDITH L. REITER
Trial Attorneys
Enforcement & Affirmative Litigation Branch
Civil Division, U.S. Department of Justice
450 5th Street, NW, Suite 6400-South
Washington, DC 20001
Phone: 202-598-7331 (Mendes)
D.C. Bar Number: 90028813 (Mendes)
Phone: 202-718-0471 (Reiter)
Illinois Bar Number: 6325095 (Reiter)

Attorneys for Plaintiff United States of America

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA**

United States of America,

Plaintiff,

v.

REPS & Company, Inc., a California
corporation;

Ryan Pancheri, individually and as an
officer and manager of REPS &
Company, Inc.;

Brian Archibald, individually and as an
officer and manager of REPS &
Company, Inc.; and

Case No.: **'26CV5895 CAB BJW**

**COMPLAINT FOR PERMANENT
INJUNCTION, MONETARY
JUDGMENT, CIVIL PENALTY
JUDGMENT, AND OTHER
RELIEF**

DEMAND FOR JURY TRIAL

Nicholas Totagrande, individually and
as an officer and manager of REPS &
Company, Inc.,

Defendants.

Plaintiff, the United States of America, acting upon notification and referral from the Federal Trade Commission (“FTC” or “Commission”), for its Complaint alleges:

1. Plaintiff brings this action for Defendants’ violations of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and the Better Online Ticket Sales Act, 15 U.S.C. § 45c. For these violations, Plaintiff seeks relief, including a permanent injunction, monetary relief, and civil penalties, pursuant to Sections 5(m)(1)(A), 13(b), and 19 of the FTC Act, 15 U.S.C. §§ 45(m)(1)(A), 53(b), and 57b(b), and the Better Online Ticket Sales Act, 15 U.S.C. § 45c.

SUMMARY OF THE CASE

2. Since at least 2022, Defendants have used illegal means to purchase millions of tickets from Ticketmaster, AXS, and other ticket issuers for concerts, sporting events, live theater, and other live entertainment. For thousands of popular events, such as concerts of Beyonce, Luke Bryan, Post Malone, and hundreds of other musical artists, music festivals, stand-up comedy shows, professional and collegiate sporting events, rodeo competitions, Broadway shows, and touring theater productions, Defendants’ purchases have regularly exceeded the maximum number of tickets a single consumer is allowed to buy.

3. Defendants use multiple methods to perpetrate their scheme, including (i) opening thousands of Ticketmaster, AXS, and other ticket issuers’ accounts under the names of employees or third parties and connecting them to Defendants’ virtual credit card accounts and phone numbers; and (ii) proxy IP addresses, Virtual Private

1 Networks (“VPNs”), and multi-session browsers to mask the locations and
2 identities of Defendants’ ticket purchasing employees and agents. These tactics
3 allow Defendants to circumvent security measures, access control systems, or other
4 technological controls or measures on ticket issuers’ websites and apps that would
5 have otherwise blocked or prevented Defendants from buying more tickets than are
6 permitted by posted ticket purchase limits.

7 4. The events Defendants target for their ticket purchase and resale
8 scheme are events in high demand where the resale price on the secondary market
9 is likely to exceed the face value of the ticket. For many of these events, ticket
10 issuers limit ticket purchases to between four and eight tickets per buyer, sometimes
11 at the request of the performing artist. Defendants’ business model is predicated on
12 identifying events for which tickets will be in high demand and buy up tickets for
13 those events before ordinary consumers can, which they do by using teams of
14 purchasers primarily located outside the United States. Defendants use analytics
15 software and data scraping to track information such as artists’ popularity and tour
16 information, and they monitor secondary marketplace trends to determine which
17 events are likely to sell out and what tickets are likely to be the most profitable.

18 5. Between January 2022 and October 2025, Defendants purchased more
19 than eight tickets from Ticketmaster and AXS for at least 83,000 separate events,
20 spending over \$1.3 billion and amassing over 18.5 million tickets for those events.
21 Defendants then resold these tickets on secondary marketplaces, such as StubHub,
22 Vivid Seats, SeatGeek, Gametime, Ticket Network, and Ticketmaster’s resale
23 marketplace, at a significant mark-up, making at least \$120.8 million in profit.

24 6. Defendants’ actions injured consumers who otherwise may have been
25 able to purchase those tickets in the first instance from ticket issuers at lower prices.
26 By circumventing ticket issuers’ security measures, access control systems, or other
27 technological controls or measures to buy tickets, and then selling or offering to sell
28

1 those tickets, Defendants have violated and continue to violate the Better Online
2 Ticket Sales Act and Section 5 of the FTC Act.

3 JURISDICTION AND VENUE

4 7. This Court has subject matter jurisdiction pursuant to 28 U.S.C.
5 §§ 1331, 1337(a), 1345, and 1355.

6 8. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(2), (c)(1),
7 (c)(2), and (d), 1395(a), and 15 U.S.C. § 53(b).

8 DEFENDANTS

9 9. Defendant REPS & Company, Inc. (“REPS”), is a California
10 corporation with its principal place of business at 4141 Jutland Drive, Suite 332,
11 San Diego, CA 92117. REPS transacts or has transacted business in this District and
12 throughout the United States. At all times relevant to this Complaint, acting alone
13 or in concert with others, REPS has purchased and then advertised, marketed,
14 distributed, or sold event tickets to consumers throughout the United States.

15 10. Defendant Ryan Pancheri is the Chief Executive Officer (“CEO”) of
16 REPS. At all times relevant to this Complaint, acting alone or in concert with others,
17 he has formulated, directed, controlled, had the authority to control, or participated
18 in the acts and practices of REPS, including the acts and practices described in this
19 Complaint. As CEO, Pancheri supervises all of REPS’s operations and, in particular,
20 technology development and maintenance, data analytics and reporting, purchasing,
21 inventory processing, pricing, fulfillment, accounting, and human resources.
22 Pancheri manages the processes for identifying ticket purchasing opportunities, the
23 ticket purchasing process, and ticket resale. He also has participated in purchasing
24 tickets on behalf of REPS. Pancheri, in connection with the matters alleged herein,
25 transacts or has transacted business in this District and throughout the United States.

26 11. Defendant Brian Archibald is the President and previously was the
27 Chief Operating Officer (“COO”) of REPS. At all times relevant to this Complaint,
28

1 acting alone or in concert with others, he has formulated, directed, controlled, had
 2 the authority to control, or participated in the acts and practices of REPS, including
 3 the acts and practices described in this Complaint. As President, Archibald oversees
 4 the process of identifying which tickets REPS should buy (in what REPS refers to
 5 as its “brokerage”), including technology development and maintenance, data
 6 analytics and reporting, purchasing, inventory processing, pricing, fulfillment,
 7 accounting, and human resources. Archibald manages the processes for identifying
 8 ticket purchasing opportunities, the ticket purchasing process, and ticket resale, and
 9 he monitors news relevant to the resale ticket industry and participates with industry
 10 groups. Archibald, in connection with the matters alleged herein, transacts or has
 11 transacted business in this District and throughout the United States.

12 12. Defendant Nicholas Totagrande is the COO of REPS. At all times
 13 relevant to this Complaint, acting alone or in concert with others, he has formulated,
 14 directed, controlled, had authority to control, or participated in the acts and practices
 15 of REPS, including the acts and practices described in this Complaint. As COO,
 16 Totagrande oversees ticket operations, including ticket purchasing, listing for resale,
 17 and distribution. Totagrande resides in this District and, in connection with the
 18 matters alleged herein, transacts or has transacted business in this District and
 19 throughout the United States.

20 **COMMERCE**

21 13. At all times relevant to this Complaint, Defendants have maintained a
 22 substantial course of trade in or affecting commerce, as “commerce” is defined in
 23 Section 4 of the FTC Act, 15 U.S.C. § 44.

24 **THE BETTER ONLINE TICKET SALES ACT**

25 14. The Better Online Ticket Sales Act makes it unlawful for any person
 26 to:
 27
 28

1 A. “circumvent a security measure, access control system, or other
2 technological control or measure on an Internet website or online
3 service that is used by the ticket issuer to enforce posted event ticket
4 purchasing limits or to maintain the integrity of posted online ticket
5 purchasing order rules,” or

6 B. “sell or offer to sell any event ticket in interstate commerce obtained
7 in violation of [the Better Online Ticket Sales Act] if the person
8 selling or offering to sell the ticket either (i) participated directly in
9 or had the ability to control the conduct in violation of [the Better
10 Online Ticket Sales Act]; or (ii) knew or should have known that the
11 event ticket was acquired in violation of [the Better Online Ticket
12 Sales Act].” 15 U.S.C. § 45c(a)(1)(B).
13

14 15. The Better Online Ticket Sales Act defines an “event” to mean “any
15 concert, theatrical performance, sporting event, show or similarly scheduled
16 activity, taking place in a venue with a seating or attendance capacity exceeding 200
17 persons that—(A) is open to the general public; and (B) is promoted, advertised, or
18 marketed in interstate commerce or for which event tickets are generally sold or
19 distributed in interstate commerce.” 15 U.S.C. § 45c note, Pub. L. 114-274, § 3.

20 16. The Better Online Ticket Sales Act defines “ticket issuer” to mean “any
21 person who makes tickets available, directly or indirectly, to the general public, and
22 may include—(1) the operator of the venue; (2) the sponsor or promoter of an event;
23 (3) a sports team participating in an event or a league whose teams are participating
24 in an event; (4) a theater company, musical group, or similar participant in an event;
25 and (5) an agent for any such person.” 15 U.S.C. § 45c note, Pub. L. 114-274, § 3.
26
27
28

1 17. A violation of the Better Online Ticket Sales Act is “a violation of a
2 rule defining an unfair or a deceptive act or practice under Section 18(a)(1)(B) of
3 the FTC Act (15 U.S.C. § 57a(a)(1)(B)).” 15 U.S.C. § 45c(b)(1). Thus, pursuant to
4 Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the Better
5 Online Ticket Sales Act is an unfair or deceptive act or practice in or affecting
6 commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

7 **DEFENDANTS’ CIRCUMVENTION OF TICKET ISSUERS’**
8 **SECURITY CONTROL MEASURES ON TICKET LIMITS**
9 **OR OTHER PURCHASE ORDER RULES**

10 18. REPS is a ticket broker. Its business involves purchasing tickets from
11 ticket issuers and then reselling those tickets to consumers on the secondary
12 marketplace at a higher price.

13 19. Since 2022, and continuing through the present, Defendants have
14 purchased over 18.6 million tickets from ticket issuers Ticketmaster and AXS
15 (through more than 3.1 million ticket purchasing transactions). For at least 83,500
16 events, Defendants purchased more than eight tickets, spending over \$1.3 billion to
17 amass over 18.5 million tickets for these events, and making at least \$120.8 million
18 in profit for reselling these tickets on the secondary marketplace.

19 20. Ticketmaster is a ticket issuer and seller that has implemented security
20 measures, access control systems, or other technological controls or measures on its
21 websites and app to enforce posted event ticket purchase limits and to maintain the
22 integrity of posted online ticket purchasing order rules.

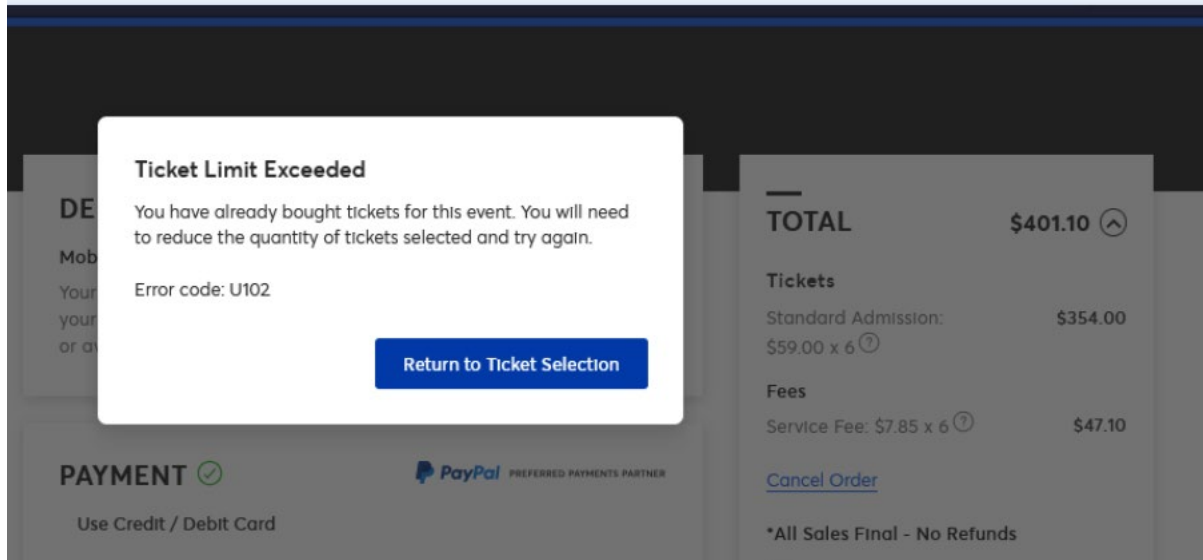
23 21. From January 2021 to at least July 2025, Ticketmaster maintained a
24 “Purchase Policy” that was posted on its website and set forth rules that “applie[d]
25 to any purchases on our Site made on or after January 1, 2021.” Section 7 of this
26 purchase policy, titled “Number of Tickets or ‘Ticket Limits,” stated that ticket
27 limits were imposed “to discourage unfair ticket buying practices.” This provision
28 specifically required that “each account” used to purchase tickets “be linked to a

1 unique individual[] and must contain valid and verifiable information” and
2 prohibited the use of multiple accounts “to circumvent or exceed published ticket
3 limits.” Section 7 further stated that tickets cancelled because the purchaser violated
4 posted ticket limits “may be refunded at face value (excluding fees),” and “[t]his
5 includes orders associated with the same name, e-mail address, billing address,
6 credit card number, or other information.” Section 13 of this policy stated that ticket
7 orders placed via accounts with false or misleading information, including false or
8 misleading information related to “name, address, email address, phone number, IP
9 address, or other account or billing information,” were subject to cancellation.

10 22. Ticketmaster’s current purchase policy, which became effective on
11 August 12, 2025, also provides that “[t]icket limits combat unfair ticket buying
12 practices” and “[u]sing multiple accounts, payment methods, email addresses, home
13 addresses, or false information, or engaging in any behavior to circumvent the ticket
14 limit or transfer restrictions, is prohibited.”

15 23. Ticketmaster’s website and app automatically prevent a single
16 Ticketmaster accountholder from adding to their cart, or purchasing, more tickets
17 than the posted limit in a single transaction. Ticketmaster uses a drop-down menu
18 that allows the purchaser to select only up to the posted ticket limit. Users that are
19 attempting to make a purchase in excess of a ticket limit will encounter an error
20 message, which Defendants refer to as a “limit error.”

21 24. For example, Ticketmaster has displayed the following message to
22 REPS employees and agents attempting to purchase tickets:
23
24
25
26
27
28



25. AXS is also a ticket issuer and seller that has implemented security measures, access control systems, or other technological controls or measures on its websites to enforce posted event ticket purchase limits and to maintain the integrity of posted online ticket purchasing order rules.

26. AXS maintains a “Purchase Agreement” on its website that has been effective since at least August 2021 (last updated on June 10, 2025) and that “appl[ies] to all listings and transactions . . . and sale or use of tickets . . . whether issued by AXS” or its clients (*i.e.*, the venue or event promoter).

27. Within this purchase agreement, there is a section titled “Limits on Tickets Per Customer,” which states:

In an effort to give all interested customers an opportunity to purchase tickets to an event or other items via the Service, our Clients often set limits on the number of seating and/or parking rights, or tickets one customer or household is allowed to purchase. You will be advised of any such limits during the purchase process, or by a system limitation on the number of tickets you may purchase during your online session. Tickets purchased for an event during multiple online sessions on the

1 Service may be totaled to ensure that any limitations imposed by
2 the Client is not exceeded. Exceeding these limits may result in
3 cancellations of orders without notice.

4 28. AXS also has “Terms of Use” that prohibit users from: “engag[ing] in
5 fraudulent or illegal activity, including without limitation . . . bulk purchasing in
6 violation of posted limits, ticket speculation or resale in violation of applicable law
7 or venue policies.”

8 29. Other ticket issuers and sellers have implemented similar policies, as
9 well as security measures, access control systems, or other technological controls
10 or measures on their websites to enforce posted event ticket purchase limits and to
11 maintain the integrity of posted online ticket purchasing order rules.

12 30. When purchasing tickets from ticket issuers, Defendants have
13 regularly circumvented their security measures, access control systems, and other
14 technological controls by, among other things, using: (i) thousands of ticket
15 purchasing accounts created with names, addresses, or phone numbers belonging to
16 someone other than the ticket purchaser, and connected to virtual credit card
17 accounts and phone numbers controlled by REPS; and (ii) computer software and
18 technology designed to facilitate such purchases, including IP proxy services to
19 utilize multiple IP addresses.

20 31. Ticket issuers that have detected that Defendants are exceeding
21 purchase limits or circumventing their technological controls have prevented, or
22 “blocked,” Defendants from completing a ticket purchase, including by displaying
23 error messages indicating that Defendants exceeded the ticket limit or that their
24 purchase activity was not typical. In thousands of instances, when the ticket issuer
25 has determined that Defendants exceeded ticket limits or otherwise engaged in
26 behavior not permitted by the issuer, the ticket issuer has canceled the ticket
27 purchase.

32. Much of Defendants' business operation revolves around circumventing ticket issuer ticket limits and other controls. For example, Defendants have created and maintained an "Error Bible" that they use to track Ticketmaster error codes and messages that Defendants encounter when attempting to circumvent Ticketmaster's security controls or technology measures. The Error Bible instructs Defendants' employees and agents on how to resolve or workaround Ticketmaster's ticket limit controls, and they have developed and refined standard operating procedures for troubleshooting and bypassing ticket limits on Ticketmaster's website.

33. By their actions, Defendants have been able to purchase tickets in greater volume than a consumer who is abiding by posted ticket purchase limits and not circumventing security measures, access control systems, or other technological controls or measures on ticket issuers' websites. Defendants have later resold for a profit or offered to resell most, if not all, of the tickets they purchased on secondary marketplaces.

34. Since at least 2022, Defendants have routinely circumvented ticket issuers' controls to purchase tickets in excess of ticket purchasing limits for thousands of events and resold tickets to these events on the secondary marketplace at a significant profit. Because Defendants mainly target and harvest tickets most likely to sell out and generate a high demand in the secondary marketplace, consumers that purchase the tickets Defendants resell often pay a significant markup.

35. As an example, from just one concert on Beyonce's Renaissance tour at Arrowhead Stadium on October 1, 2023, Defendants used at least 1,300 accounts to purchase 7,624 tickets through Ticketmaster. The ticket purchase limit for that concert was between four and eight. Defendants made approximately \$833,323 in profit by reselling those tickets.

1 36. For a Pitbull concert at the Empower FCU Amphitheater on September
2 7, 2024, Defendants used at least 700 accounts to purchase 5,430 tickets through
3 Ticketmaster. That venue holds an estimated 17,500 people, and Defendants
4 purchased and resold nearly one-third of that capacity, making approximately
5 \$120,109 in profit.

6 37. These events are only two examples of the thousands of different
7 events where Defendants purchased tickets in excess of the posted ticket purchase
8 limits.

9 **DEFENDANTS USE MULTIPLE ACCOUNTS TO CIRCUMVENT**
10 **TICKET ISSUERS' CONTROLS TO FURTHER THEIR ILLEGAL**
11 **TICKET SCALPING SCHEME**

12 38. Since at least 2022, Ticketmaster and other ticket issuers have
13 maintained security measures, access control systems, or other technological
14 controls or measures on their websites and apps designed to prevent individuals
15 from purchasing more tickets than allowed under their posted event ticket limits.

16 39. Some of these security measures or controls used by the ticket issuers
17 are intended to verify an account user's personal information to ensure, among other
18 things, that a purchase falls within posted purchase limits and that a person is not
19 using multiple accounts to purchase tickets. The account verifying information
20 typically includes: (a) the account user's name; (b) billing and email addresses; and
21 (c) the IP address and digital cookies associated with the purchase. Ticket issuers
22 and sellers, such as Ticketmaster, also monitor the credit card numbers used by the
23 purchaser to ensure that a person is not using multiple accounts to purchase tickets
24 to the same event.

25 40. Defendants have routinely circumvented these account verification
26 security measures or controls by using thousands of individual ticket issuer
27 accounts, thousands of credit card numbers generated through virtual credit card
28

1 accounts, thousands of phone numbers, and IP proxy services and multi-session
2 browsers to enable Defendants to mask the identity and location of the account user.

3 41. REPS employs a team of ticket purchasers, most of whom are based
4 in the Philippines, to purchase tickets on its behalf using accounts that REPS
5 controls and that are not linked to a unique individual, as required by Ticketmaster's
6 policies. REPS trains the purchasers and evaluates them to assess their purchasing
7 speed and facility using multiple accounts and the other tools REPS provides.

8 42. To create accounts for its purchasers to use, REPS enters into "power
9 of attorney" agreements with its employees and third-party partners that authorize
10 REPS to use that person's name and address to establish an account with ticket
11 issuers. These individuals also authorize REPS to "converse with websites such as
12 Ticketmaster.com" using their name.

13 43. When creating ticket issuer accounts using these individuals' names
14 and addresses, REPS provides information unrelated to the authorizing individuals,
15 like the contact information (email address and phone number) and credit card
16 information for the account. Using variations on each person's name and numerous
17 email domains, REPS creates multiple email addresses for each person. In turn, it
18 creates multiple ticket issuer accounts using an amalgamation of each person's
19 information and information supplied by REPS. REPS has created as many as 40
20 accounts using one individual's name and address. On average it creates 19 accounts
21 per person. REPS has also used ticket industry service providers such as Broker
22 Genius Inc. (doing business as "Automatiq") to fully automate the creation of
23 hundreds of ticket issuer accounts. REPS relies on Automatiq for a variety of other
24 ticket sale-related services, for example integrating with secondary ticket
25 marketplaces like Vivid Seats and automatically listing tickets for sale.

26 44. In response to receiving "limit error" messages from Ticketmaster, and
27 to avoid experiencing this error, Defendants have created new accounts or modified
28 account information, such as the spelling of an address. REPS carefully instructs its

1 employees and agents how to do so. Internal instructions for account creation
2 explain: “In order to combat the Limit Error problem, we make modifications to the
3 base address and use the new modified address to create a new [Ticketmaster
4 account].” In one instance in March 2024, after purchasers using certain accounts
5 encountered limit errors, another employee notified Defendant Totagrande that they
6 “slightly modified the address, and they were successful in purchasing.”

7 45. Defendants’ creation and use of multiple accounts is aided by the use
8 of thousands of SIM cards across multiple SIM banks or boxes—devices that house
9 dozens of SIM cards at a time. Defendants have used SIM banks or trays to facilitate
10 the receipt and automated retrieval of account verification codes sent by ticket
11 issuers to the many phone numbers associated with Defendants’ ticket-purchasing
12 accounts, frustrating the purpose of the ticket issuers’ account verifications.

13 46. Defendants also have used their supply of virtual credit cards to replace
14 the credit card information on accounts when they suspect an account block is
15 related to that account information. Defendants understand that ticket issuers and
16 sellers like Ticketmaster use credit card information to link accounts in order to
17 block accounts from exceeding ticket limits. For example, when discussing whether
18 REPS could link the same virtual credit card to multiple purchasing accounts,
19 Defendant Pancheri expressed concern that Ticketmaster would recognize
20 purchases on different accounts that used the same credit card as tickets purchased
21 on the same account, and it would not allow the purchases or would cancel them.

22 47. Defendants’ internal documents reveal that Defendants strive to
23 “maximize purchasing efficiency” by “ensuring that accounts in use are less likely
24 to be flagged, allowing for smoother and faster transactions,” and that Defendants
25 aim to have “non-obvious accounts” or “clean” accounts that will not be detected
26 by ticket issuers. To that end, Defendants routinely test accounts to assess
27 purchasing success rates, *i.e.*, whether attempted purchases are successfully
28 completed or are somehow blocked by the ticket issuer. Through this testing,

1 Defendants evaluate, for example, how the age of an account impacts the number
2 of limit errors, or whether the domain in an account email address results in that
3 account being blocked. This testing has informed Defendants' strategies for
4 continuously creating new accounts and rotating accounts in and out of use to "keep
5 usage patterns less predictable and reduce the frequency of limit errors."

6 48. For example, in October 2023, Defendants identified that Ticketmaster
7 "released some sort of new security 'thing' which is causing accounts to be unusable
8 for checkout." Defendant Totagrande explained to his colleagues that they were
9 "pinpointing the factors we think influence 'getting blocked' and are pushing
10 backup accounts to compensate." Totagrande said he hoped "we find the cause or
11 [Ticketmaster] stops whatever they are currently doing" and if solving it is not
12 straightforward "we have to immediately shift all efforts to solving this."

13 49. At all times relevant to the Complaint, Defendants have known that if
14 they purchased tickets using only their true names, addresses, and other valid
15 account information, then ticket issuers' security measures could prevent them from
16 purchasing tickets in excess of ticket purchase limits.

17 **DEFENDANTS MASK THEIR IP ADDRESSES TO CIRCUMVENT**
18 **TICKET ISSUERS' CONTROLS**

19 50. Since at least 2022, Ticketmaster and other ticket issuers have
20 maintained security measures, access control systems, or other technological
21 controls or measures on their websites and apps designed to prevent or block ticket
22 purchasers from making multiple purchases for the same event using the same IP
23 address. An IP address is a unique string of numbers separated by periods that
24 Ticketmaster uses to identify an electronic device or affiliated electronic devices
25 making purchases. Ticketmaster uses IP detection systems to enforce posted event
26 ticket purchase limits and to maintain the integrity of their posted online ticket
27 purchasing order rules. Other ticket issuers, like AXS, have also implemented
28

1 similar security measures to prevent ticket purchasers from exceeding the event
2 ticket purchasing limits.

3 51. Since at least 2022, Defendants have taken steps to conceal their IP
4 addresses when making ticket purchases. Defendants have used and provided their
5 employees and agents with virtual private networks (“VPNs”) and rotating IP proxy
6 services, such as PrimoBrowser, Multilogin, and Insomniac, which allow
7 Defendants to hide their actual IP addresses from ticket issuers. Defendants also use
8 multi-session browsers, which are specialized browsers or browser extensions that
9 allow individuals to open multiple independent internet browsing sessions within
10 one application. These multi-session browsers allow users to assign specific proxy
11 services to individual sessions to bypass geo-restrictions or bans from the website’s
12 host. PrimoBrowser, for example, promotes its software as a “Multi-Session
13 Browser Designed for [Ticket] Resellers” that enable clients to “[r]un multiple
14 sessions and accounts with unique proxies in a single browser.” REPS describes
15 Multilogin as a tool that “allows multiple users to login into one account and show
16 up as if they are using one device. This prevents our purchasing accounts from
17 triggering reset passwords, being flagged by Ticketmaster or other marketplaces . .
18 .” Using these services, Defendants and their agents can mask their actual IP
19 addresses from ticket issuers and avoid “limit errors” and other ticket issuer
20 controls.

21 52. Defendants and their employees and agents use multi-session browsers
22 with IP proxy services to appear multiple times in event sales queues using multiple
23 accounts and from purportedly different physical locations. For example, in
24 February 2025, REPS purchasers on average were queuing in 8 browser tabs during
25 the initial on sale period for events, and in some instances, purchasers were able to
26 open at least 15 internet browser tabs simultaneously. These tools also allow REPS
27 purchasers outside the United States to purchase tickets that issuers intend to only
28 make accessible to users inside the United States.

53. Defendants have routinely tested these tools to determine which have a higher “success rate” for purchasing tickets and to inform their strategy for how to purchase tickets, as they understand that the effectiveness of proxies “influence whether or not a purchaser gets blocked by [Ticketmaster].” In particular, Defendants assess how REPS purchasers can use proxy services to successfully make purchases while signed into multiple accounts. REPS aims to “ensure all purchasers have access to reliable, working proxies to minimize downtime from blocks” and increase purchasing speed.

54. Defendants have identified that changing the proxy is a useful troubleshooting method when purchasers encounter limit errors or other blocks on purchases. For example, in April 2024, one purchaser using 20 accounts was encountering “a lot of limit errors” but “managed to troubleshoot by changing the proxy that she was using.” Despite the errors, in just two hours that purchaser bought 128 tickets in 20 transactions.

55. Around March 2025, Defendants determined that AXS implemented a new verification measure that blocked some REPS purchasers. The message displayed to users who were being blocked explained that users could take various steps to resolve this block, including disabling a VPN. After REPS developed a way to bypass the block, its purchasers encountered a pop-up message requiring the user to check a box to “verify you are a human.” REPS assessed that this “new blocker” caused a 40% slowdown of its purchases, which it determined it could avoid by using a proxy IP address.

56. In September 2025, Defendants learned that Ticketmaster had recently implemented a measure to track IP addresses used with an account, and if the IP address changed too frequently, the account would be flagged and suspended. Soon thereafter, in strategic planning for 2026, Defendant Totagrande identified a goal to “reduce transaction failure, suspended errors, and account blocks by keeping the same proxy/IP tied to each account.”

1 57. By using multi-session browsers and IP proxy services, Defendants
2 have been able to increase the odds of purchasing as many event tickets as they can
3 from ticket issuers. By hiding their true IP addresses from ticket issuers, Defendants
4 have circumvented security measures, access control systems, or other
5 technological controls or measures that ticket issuers used on their websites to
6 enforce posted event ticket purchase limits, or to maintain the integrity of posted
7 online ticket purchasing order rules.

8 58. At all times relevant to the Complaint, Defendants have known that if
9 they purchased tickets using only their true IP addresses, then ticket issuers' security
10 measures could prevent them from making ticket purchases.

11 **DEFENDANTS' KNOWLEDGE OF THEIR VIOLATIONS OF THE**
12 **BETTER ONLINE TICKET SALES ACT**

13 59. Defendants have been aware of the Better Online Ticket Sales Act
14 since its enactment in December 2016, nearly a year before the formation of REPS,
15 and have monitored its enforcement while continuing to violate the Act.

16 60. In 2022, on a questionnaire related to a financial audit signed by
17 Defendant Archibald, REPS listed the Better Online Ticket Sales Act as a law
18 applicable to the company. REPS has required partner companies to agree to comply
19 with the Better Online Ticket Sales Act, and it likewise has represented to vendors
20 and lenders that it complies with the Act.

21 61. In July 2025, Defendants became aware of the FTC's investigation of
22 ticket broker Key Investment Group when that company sued the FTC for a
23 declaratory judgment. The FTC's complaint against ticket broker Key Investment
24 Group was filed on August 18, 2025. *FTC v. Key Investment Group LLC*, 1:25-cv-
25 02716-CJC (D. Md. Aug. 18, 2025). The complaint alleges that Key Investment
26 Group used unlawful tactics to exceed ticket purchasing limits, in violation of the
27 Better Online Ticket Sales Act.

62. In September 2025, Defendants became aware of the FTC's law enforcement action against Live Nation and its subsidiary Ticketmaster, *FTC v. Live Nation Ent. Inc.*, 2:25-cv-08884 (C.D. Cal. Sept. 18, 2025). The complaint alleges that Ticketmaster violated the Better Online Ticket Sales Act.

63. Despite knowing of the Better Online Ticket Sales Act and its enforcement, Defendants continue to operate their ticket brokering business as they have since 2017, using numerous ticket issuer accounts, concealed IP addresses, and other means to obtain tickets by circumventing security measures, access control systems, or other technological controls or measures on Ticketmaster's websites and then selling or offering to sell those tickets in interstate commerce.

PLAINTIFF HAS REASON TO BELIEVE THAT DEFENDANTS ARE VIOLATING AND WILL CONTINUE TO VIOLATE THE BETTER ONLINE TICKET SALES ACT AND THE FTC ACT

64. Upon information and belief, Defendants are violating or are about to violate the FTC Act and the Better Online Ticket Sales Act: Defendants have been aware since at least December 2016 of the Better Online Ticket Sales Act yet Defendants continue to circumvent security measures, access control systems, or other technological controls or measures on Ticketmaster, AXS, and other ticket issuers' websites.

COUNT I: VIOLATIONS OF THE BETTER ONLINE TICKET SALES ACT AND THE FTC ACT

65. Paragraphs 1 through 64 are incorporated as if set forth herein.

66. In numerous instances, Defendants have engaged in unfair or deceptive acts or practices by buying multiple event tickets through circumventing a security measure, access control system, or other technological controls or measures that Ticketmaster or other ticket issuers have used on their websites or apps to enforce posted event ticket limits or to maintain the integrity of posted online ticket purchasing order rules. Defendants have subsequently sold or offered

1 to sell in interstate commerce the tickets they have obtained in this manner, typically
2 at significantly more than the face value of these tickets.

3 67. Defendants know that the Better Online Ticket Sales Act prohibits
4 these acts or practices.

5 68. Defendants' acts or practices violate the Better Online Ticket Sales
6 Act and the FTC Act.
7

8 **CONSUMER INJURY**

9 69. Consumers are suffering, have suffered, and will continue to suffer
10 substantial injury as a result of Defendants' violations of the FTC Act and the Better
11 Online Ticket Sales Act. Absent injunctive relief by this Court, Defendants are likely
12 to continue to injure consumers and harm the public interest.

13 **CIVIL PENALTIES**

14 70. Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A),
15 authorizes this Court to award civil penalties for each violation of the Better Online
16 Ticket Sales Act, 15 U.S.C. § 45c.

17 71. Defendants violated the Better Online Ticket Sales Act, 15 U.S.C.
18 § 45c, with actual knowledge or knowledge fairly implied on the basis of objective
19 circumstances as required by Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. §
20 45(m)(1)(A).
21
22
23
24
25
26
27
28

PRAYER FOR RELIEF

Wherefore, Plaintiff requests that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act and the Better Online Ticket Sales Act in accordance with Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and Section 2(b) of the Better Online Ticket Sales Act, 15 U.S.C. § 45c(b);

B. Award monetary and other relief within the Court's power to grant;

C. Impose civil penalties for each violation of the Better Online Ticket Sales Act, in accordance with Section 2(b) of that Act, 15 U.S.C. § 45c(b), and Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A); and

D. Award any additional relief as the Court determines to be just and proper.

1 Dated: October 15, 2026

Respectfully submitted,

2 BRETT A. SHUMATE
3 Assistant Attorney General
4 Civil Division

5 CODY M. POPLIN
6 Deputy Assistant Attorney General

7 HILARY K. PERKINS
8 Director

9 LISA K. HSIAO
10 Deputy Director

11 MARCUS P. SMITH
12 Assistant Director

13 Of Counsel:

14 Rebecca Plett
15 Molly Rucki
16 Benjamin R. Davidson
17 Federal Trade Commission
18 600 Pennsylvania Avenue NW
19 Washington, DC 20580
20 rplett@ftc.gov | (202) 326-3664
21 mrucki@ftc.gov | (202) 326-3774
22 bdavidson@ftc.gov | (202) 326-3055

/s/ Austin T. Mendes
AUSTIN T. MENDES
MEREDITH L. REITER
Trial Attorneys
Enforcement & Affirmative Litigation
Branch
Civil Division, U.S. Department of
Justice
450 5th Street, NW, Suite 6400-South
Washington, DC 20001
Phone: 202-598-7331 (Mendes)
Austin.T.Mendes@usdoj.gov
Phone: 202-718-0471 (Reiter)
Meredith.L.Reiter@usdoj.gov

23 *Attorneys for Plaintiff United States of*
24 *America*