UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

v.

CARTISIM CORPORATION, formerly known as Ebrani Corporation and Ebrani Enterprises, a corporation, and

SIMON EBRANI, individually and as an officer of Cartisim Corporation,

Defendants.

Civil Action No.
21-CV-212

COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF

Plaintiff, the United States of America, by its undersigned attorneys, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("FTC") pursuant to Section 16(a)(1) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 56(a)(1), for its Complaint alleges:

1. Plaintiff brings this action under Sections 5(m)(1)(A), 13(b), 16(a), and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(m)(1)(A), 53(b), 56(a), and 57b and Section 2 of the Better Online Ticket Sales Act ("the BOTS Act"), 15 U.S.C. § 45c, to obtain monetary civil penalties, permanent injunctive relief, and other relief for Defendants' acts or practices in violation of Section 2(a) of the BOTS Act, 15 U.S.C. § 45c(a) and Section 5 of the FTC Act, 15 U.S.C. § 45(a).

SUMMARY OF THE CASE

2. Between January 1, 2017 and the present date, Defendants have used ticket bots and other technology to gain access to tens of thousands of tickets for performances and events, including concerts and sporting events. Defendants' purchases exceeded posted ticket limits to

many popular events, like Elton John concerts. Defendants also have used hundreds of fictitious Ticketmaster accounts, multiple credit cards (including some in the names of fictitious individuals), and proxy or spoofed IP addresses to bypass, trick, or otherwise avoid security measures, access control systems, or other technological controls or measures on Ticketmaster's websites, that would have otherwise blocked or prevented them from obtaining so many tickets. Defendants then have resold or have attempted to resell the tickets on secondary ticketing websites. Defendants have made more than $3.8 million in revenue selling the tickets they obtained from Ticketmaster on secondary markets—often at a significant price markup. Their actions prejudiced consumers, who otherwise may have been able to purchase those tickets directly from Ticketmaster at a lower price. By their actions, Defendants have violated the BOTS Act and the FTC Act.

JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), 1345.

4. Venue is proper in this district under 28 U.S.C. § 1391(b)(1), (b)(2), (b)(3), (c)(1), (c)(2), (c)(3) and (d), and 1395(a), and 15 U.S.C. § 53(b).

DEFENDANTS

5. Defendant Cartisim Corporation, formerly known as Ebrani Corporation and Ebrani Enterprises, ("Cartisim") is a New York corporation with its principal place of business at 747 Middle Neck Road, Great Neck, NY 11024. Cartisim transacts or has transacted business in this District and throughout the United States.

6. Defendant Simon Ebrani ("Simon Ebrani") is the owner and president of Cartisim. At all times material to this Complaint, acting alone or in concert with others, he has formulated,

directed, controlled, or had the authority to control or participated in the acts and practices of Cartisim, including the acts and practices set forth in this Complaint. Simon Ebrani resides in New York, and, in connection with the matters alleged herein, transacts or has transacted business in this district.

7. On July 26, 2016, Defendants signed an Assurance of Discontinuance with the New York Attorney General relating to, among other things, their use of ticket bots. The New York Attorney General alleged, among other things, that Defendants violated New York state law by using automated ticket purchasing software, or any machine, device, or computer program that navigates or runs automated tasks on retail ticket purchasing websites in order to bypass security measures to purchase tickets. Under the Assurance of Discontinuance, Defendants agreed "not to utilize automated ticket purchasing software, including Bots, in order to bypass security measures to purchase tickets to events in New York, or to maintain an interest in or maintain control over the operation of automated ticket purchasing software to bypass security measures to purchase tickets."

COMMERCE

8. At all times material to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

THE BOTS ACT

9. Under the BOTS Act, it is unlawful for any person to "circumvent a security measure, access control system, or other technological control or measure on an Internet website or online service that is used by the ticket issuer to enforce posted event ticket limits or to maintain the integrity of posted online ticket purchasing order rules." 15 U.S.C. § 45c(a)(1).

10. The BOTS Act defines an "event" to mean "any concert, theatrical performance, sporting event, show, or similarly scheduled activity, taking place in a venue with a seating or attendance capacity exceeding 200 persons that—(A) is open to the general public; and (B) is promoted, advertised, or marketed in interstate commerce or for which event tickets are generally sold or distributed in interstate commerce."

11. A violation of the BOTS Act is "a violation of a rule defining an unfair or a deceptive act or practice under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B))." 15 U.S.C. § 45c(b)(1). Thus, pursuant to Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the BOTS Act is an unfair or deceptive act or practice in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

DEFENDANTS CIRCUMVENTED SECURITY MEASURES, ACCESS CONTROL SYSTEMS, OR TECHNOLOGICAL CONTROLS OR MEASURES ON TICKETMASTER'S WEBSITES

12. Cartisim is a ticket reseller. Its primary business involves purchasing tickets on from primary ticket sellers, and then reselling the tickets to consumers on secondary ticketing websites.

13. Simon Ebrani, as the President of Cartisim, was involved in selecting the tickets for purchase and arranging for their resale.

14. Between January 1, 2017 and the present date, Defendants have made more than 9,088 Ticketmaster ticket purchases. They obtained more than 24,478 tickets from these purchases.

15. Ticketmaster is a ticket issuer 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.

16. In many instances, Defendants circumvented security measures, access control systems, and other technological controls or measures on Ticketmaster's websites by, among other things, using ticket bots and other computer software and technologies, CAPTCHA bypass or solving services, fictitious names and addresses, multiple credit card accounts (including some in the names of fictitious individuals), and IP proxies.

17. By their actions, Defendants have been able to purchase tickets far more rapidly and in a greater volume than a consumer who was not using ticket bots or otherwise circumventing security measures, access control systems, or other technological controls or measures on Ticketmaster's websites.

18. Defendants later resold many of the tickets on secondary ticketing websites, for a profit.

DEFENDANTS' USE OF TICKET BOTS TO CIRCUMVENT SYSTEMS OR CONTROLS ON TICKETMASTER'S WEBSITES

19. Between January 1, 2017 and at least February 2019, in numerous instances, Defendants used an automated computer program called Tixman to purchase tickets on Ticketmaster's websites. Defendants entered information into the Tixman ticket bot about the tickets that they were interested in purchasing and the price they would pay for those tickets. The Tixman ticket bot then would search Ticketmaster's websites to see if the tickets were available to purchase. The Tixman ticket bot would automatically reserve any tickets that fit Defendants' search criteria. This reservation set aside the tickets for Defendants and blocked others from purchasing them, at least until the reservation clock expired. Defendant Simon Ebrani would then review the reserved tickets and select which tickets to purchase.

20. The Tixman ticket bot saved Defendants' credit card information and Ticketmaster account information, and automatically entered that information into Ticketmaster's websites.

Also, the Tixman ticket bot would bypass any CAPTCHAs it encountered on Ticketmaster's websites while searching for or reserving tickets on Defendants' behalf. CAPTCHA is an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart." At times, Ticketmaster used CAPTCHAs on its websites to try to ensure that visitors to its website were humans, and not automated computer programs or ticket bots.

21. Between April 2018 and at least May 2019, in many instances, Defendants also used an automated computer program called Tixdrop to purchase tickets on Ticketmaster's websites. Defendants entered information into the Tixdrop ticket bot about the tickets that they were interested in purchasing. The Tixdrop ticket bot then would repeatedly search Ticketmaster's websites to see if the tickets were available to purchase. The Tixdrop ticket bot would automatically reserve any tickets that fit Defendants' search criteria. This reservation set aside the tickets for Defendants and blocked others from purchasing them, at least until the reservation clock expired. Defendant Simon Ebrani would then review the reserved tickets and select which tickets to purchase.

22. The Tixdrop ticket bot also saved Defendants' credit card information and Ticketmaster account information, and automatically entered that information into Ticketmaster's websites. In addition, the Tixdrop ticket bot would automatically complete all CAPTCHAs that appeared on Ticketmaster's websites while it was searching for or reserving tickets at the direction of Defendants.

23. By using the Tixdrop and Tixman ticket bots, Defendants were able to purchase multiple tickets across multiple Ticketmaster accounts within seconds—something that a consumer abiding by Ticketmaster's security, access control, and other technological measures would be unable to do.

24. Defendants' use of the Tixman and Tixdrop ticket bots, along with other technologies, allowed them to circumvent security measures, access control systems, or other technological controls or measures on Ticketmaster's websites that were used by Ticketmaster to enforce posted event ticket purchase limits, or to maintain the integrity of posted online ticket purchasing order rules.

DEFENDANTS HID THEIR IP ADDRESSES TO CIRCUMVENT SYSTEMS OR CONTROLS ON TICKETMASTER'S WEBSITES

25. Between January 1, 2017 and the present date, Ticketmaster has had security measures, access control systems, or other technological controls or measures on its websites that were designed to prevent or block ticket purchasers from making multiple purchases on the same day from the same IP address. An IP address is a unique string of numbers separated by periods that Ticketmaster uses to identify a computer or affiliated computers making purchases. Ticketmaster uses this technological system to enforce posted event ticket purchase limits and to maintain the integrity of its posted online ticket purchasing order rules.

26. In many instances, between January 1, 2017 and the present date, Defendants have taken steps to conceal their IP address when making ticket purchases. For example, at times, Defendants used rotating proxy services and IP address blocks. These services allowed Defendants to hide their actual IP address from Ticketmaster and instead use a proxy IP address or the IP address of a computer or network that belongs to someone else.

27. Between January 1, 2017 and the present date, Defendants have used over 8,000 different IP addresses while making purchases on Ticketmaster's websites.

28. Defendants hid their true IP addresses from Ticketmaster because they believed it would allow them to circumvent technological controls on Ticketmaster's websites.

29. By hiding their true IP addresses from Ticketmaster, Defendants have circumvented security measures, access control systems, or other technological controls or measures on Ticketmaster's websites that were used by Ticketmaster to enforce posted event ticket purchase limits, or to maintain the integrity of posted online ticket purchasing order rules.

DEFENDANTS' USE OF FICTITIOUS NAMES, MULITIPLE TICKETMASTER ACCOUNTS, PROXY IP ADDRESES, AND MULTIIPLE CREDIT CARDS TO CIRCUMVENT SYSTEMS OR CONTROLS

30. Between January 1, 2017 and the present date, Ticketmaster also has had security measures, access control systems, or other technological controls or measures in place on its websites that were designed to prevent individuals from purchasing more tickets than is otherwise allowed under its posted event ticket limits. Among other things, these technological measures monitor the following information to verify whether the purchase fell within posted purchase limits: (a) the individual's name, (b) billing address, (c) Ticketmaster accounts, and (d) the IP address and cookies associated with the computer that made the purchase. From January 1, 2017 until or around October 2018, Ticketmaster also monitored the credit card number used by the purchaser.

31. In many instances, between January 1, 2017 and the present date, Defendants have bypassed these security measures, access control systems, or other technological controls and measures by using sham identities and addresses, multiple credit cards, multiple Ticketmaster accounts, and IP proxy services.

32. Defendants have used more than 120 Ticketmaster accounts to purchase tickets during the relevant period. Each Ticketmaster account had a unique email address.

33. Defendants typically did not open Ticketmaster accounts in their own names, but in the names of family and friends. Defendants have used more than 115 different names to open the accounts.

34. In many instances, Defendants also did not use their address as the primary address, shipping address, or billing address for their Ticketmaster accounts. Instead, they used over 110 addresses that were either fake or unrelated to their business.

35. Defendants have used more than 150 different credit cards to make purchases through their Ticketmaster accounts. In numerous instances, Defendants' Ticketmaster accounts included credit cards in the names of fictitious individuals or the names of friends and family. Defendants opened at least 26 corporate credit cards in the names of fictitious individuals or friends and family members. Defendants have used many of these credit cards to purchase tickets.

36. As discussed above, Defendants also hid from Ticketmaster the true IP addresses of the computers used by Defendants to make purchases.

37. Defendants knew that if they purchased tickets using their true names, addresses, and IP addresses, then Ticketmaster could prevent them from making all of the purchases they wished to make, or their purchases could be cancelled.

38. Defendants' use of multiple names, addresses, IP addresses, credit cards, and Ticketmaster accounts circumvented Ticketmaster's security measures, access control systems, or other technological controls or measures that were designed to prevent ticket purchasers from exceeding posted event ticket purchase limits.

PLAINTIFF HAS REASON TO BELIEVE THAT DEFENDANTS ARE VIOLATING AND WILL CONTINUE TO VIOLATE THE BOTS ACT AND THE FTC ACT

39. Based on the facts and violations of law alleged in this Complaint, Plaintiff has reason to believe that Defendants are violating or are about to violate laws enforced by the Commission, because among other things, (a) Defendants have been aware of the BOTS Act since early 2017, but continued to violate the Act; (b) Defendants continue to circumvent security measures, access control systems, or other technological controls or measures on Ticketmaster's

websites; and (c) Defendants are recidivists who continued to engage in unlawful conduct after prior enforcement action.

COUNT I - VIOLATIONS OF THE BOTS ACT AND THE FTC ACT

40. As alleged in paragraphs 1 through 39, in numerous instances, Defendants have circumvented a security measure, access control system, or other technological control or measure on Ticketmaster's websites that is used by Ticketmaster to enforce posted event ticket limits or to maintain the integrity of posted online ticket purchasing order rules.

41. Therefore, Defendants' acts or practices as set forth in paragraphs 1 through 39 violate the BOTS Act and the FTC Act.

CONSUMER INJURY

42. Consumers have suffered and will continue to suffer substantial injury as a result of Defendants' violations of the BOTS Act and the FTC Act. In addition, Defendants have been unjustly enriched as a result of their unlawful acts or practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

43. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

44. Section 19 of the FTC Act, 15 U.S.C. § 57b, and the BOTS Act authorizes this Court to grant such relief as the Court finds necessary to redress injury to consumers resulting

from Defendants' violations of the BOTS Act, including the rescission or reformation of contracts, and the refund of money.

45. Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A), as modified by Section 4 of the Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461, as amended, and as implemented by 16 C.F.R. § 1.98(d), authorizes this Court to award monetary civil penalties. From August 1, 2016 to January 21, 2018, the Court was authorized to award a penalty of up to $40,000 for each violation of the BOTS Act. *See* 16 C.F.R. § 1.98(d) (2016). From January 22, 2018 to February 13, 2019, the maximum penalty amount was $41,484 per violation, and effective February 14, 2019, the maximum penalty amount was adjusted to $42,530 per violation, pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015. *See* 16 C.F.R. § 1.98(d) (2018); 84 Fed. Reg. 3980 (Feb. 13, 2019). Defendants' violations of the BOTS Act were committed with the knowledge required by Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

46. This Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including disgorgement, to prevent and remedy any violation of the BOTS Act and the FTC Act.

PRAYER FOR RELIEF

Wherefore, Plaintiff, pursuant to Sections 5(a), 5(m)(1)(A), and 13(b) and 19 of the FTC Act, 15 U.S.C. §§ 45(a), 45(m)(1)(A), and 53(b), Section 2(a) of the BOTS Act, 15 U.S.C. § 45c(a)(1), and the Court's own equitable powers, requests that this Court:

A. Enter judgment against Defendants and in favor of Plaintiff for each violation alleged in this Complaint;

B. Enter a permanent injunction to prevent future violations of the BOTS Act by Defendants;

C. Award Plaintiff monetary civil penalties from each Defendant for every violation of the BOTS Act;

D. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies;

E. Award Plaintiff the costs of bringing this action, as well as such other and additional relief, including disgorgement, as the Court may determine to be just and proper.

Date: January 14, 2021

Respectfully submitted,

FOR THE UNITED STATES OF AMERICA

JENNIFER B. DICKEY
Acting Assistant Attorney General
Civil Division

DANIEL J. FEITH
Deputy Assistant Attorney General

GUSTAV W. EYLER
Director, Consumer Protection Branch

/s/ Benjamin A. Cornfeld
BENJAMIN A. CORNFELD
Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
P.O. Box 386
Washington, D.C. 20004
Tel: 202-598-7276
Fax: 202-514-8742
Benjamin.A.Cornfeld2@usdoj.gov

SETH D. DUCHARME
Acting United States Attorney
Eastern District of New York

/s/ Bonni J. Perlin
BONNI J. PERLIN
KEVIN YIM
Assistant U.S. Attorneys
Tel: (718) 254-6254
Tel: (718) 254-6186
bonni.perlin@usdoj.gov
kevin.yim@usdoj.gov