

AL/DMP:CRH/ICR
F. #2020R01158

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----- X

UNITED STATES OF AMERICA

DEFERRED PROSECUTION
AGREEMENT

- against -

Cr. No. 20-563 (MKB)

TICKETMASTER L.L.C.,

Defendant.

----- X

DEFERRED PROSECUTION AGREEMENT

Defendant Ticketmaster L.L.C. (the “Company”), pursuant to authority granted by the Company’s Board of Directors, reflected in Attachment B, and the United States Attorney’s Office for the Eastern District of New York (the “Office”), enter into this deferred prosecution agreement (the “Agreement”).

Criminal Information and Acceptance of Responsibility

1. The Company acknowledges and agrees that the Office will file the attached criminal information (the “Information”) in the United States District Court for the Eastern District of New York charging the Company with: (i) one count of conspiracy to commit offenses against the United States, in violation of Title 18, United States Code, Section 371, that is, to violate provisions of the Computer Fraud and Abuse Act (“CFAA”) as amended, see Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(a)(4); (ii) one substantive count of computer intrusion for commercial advantage or private financial gain, in violation of Title 18, United States Code, Section 1030(a)(2)(C); (iii) one substantive count of computer intrusion in furtherance of

fraud, in violation of Title 18, United States Code, Section 1030(a)(4); (iv) one count of conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349; and (v) one substantive count of wire fraud, in violation of Title 18, United States Code, Section 1343. In so doing, the Company: (a) knowingly waives its right to indictment on these charges, as well as all rights to a speedy trial pursuant to the Sixth Amendment to the United States Constitution; Title 18, United States Code, Section 3161; and Federal Rule of Criminal Procedure 48(b), and its rights under the statute of limitations under Title 18, United States Code, Section 3282; (b) knowingly waives any objection with respect to venue to any charges by the United States arising out of the conduct described in the Statement of Facts attached hereto as Attachment A (the “Statement of Facts”); and (c) consents to the filing of the Information, as provided under the terms of this Agreement, in the United States District Court for the Eastern District of New York. The Office agrees to defer prosecution of the Company pursuant to the terms and conditions described below.

2. The Company admits, accepts and acknowledges that it is responsible under United States law for the acts of its officers, directors, employees and agents, with respect to the conduct described in the Information and the Statement of Facts, and that the facts described in the Information and Statement of Facts are true and accurate. Should the Office pursue the prosecution that is deferred by this Agreement, the Company stipulates to the admissibility of the Statement of Facts in any proceeding by the Office, including any trial, guilty plea or sentencing proceeding, and will not contradict anything in the Statement of Facts at any such proceeding. The Company agrees that, effective as of the date the Company signs this Agreement, in any prosecution that is deferred by this Agreement, it will not dispute the Statement of Facts set forth in this Agreement, and, in any such prosecution, the Statement of Facts shall be admissible as: (a) substantive

evidence offered by the government in its case-in-chief and rebuttal case; (b) impeachment evidence offered by the government on cross-examination; and (c) evidence at any sentencing hearing or other hearing. In addition, in connection therewith, the Company agrees not to assert any claim under the United States Constitution, Rule 410 of the Federal Rules of Evidence, Rule 11(f) of the Federal Rules of Criminal Procedure, Section 1B1.1(a) of the United States Sentencing Guidelines (“USSG” or “Sentencing Guidelines”), or any other federal rule that the Statement of Facts should be suppressed or is otherwise inadmissible as evidence in any form.

Term of the Agreement

3. This Agreement is effective for a period beginning on the date on which the Information is filed and ending three (3) years from that date (the “Term”). The Company agrees, however, that, in the event the Office determines, in its sole discretion, that the Company has knowingly violated any provision of this Agreement or has failed to completely perform or fulfill each of the Company’s obligations under this Agreement, an extension or extensions of the Term may be imposed by the Office, in its sole discretion, for up to a total additional time period of one year, without prejudice to the Office’s right to proceed as provided in Paragraphs 18-21 below. Any extension of the Agreement extends all terms of the Agreement, including the terms of the reporting requirement in Attachment D (Corporate Compliance Reporting), for an equivalent period. Conversely, in the event the Office finds, in its sole discretion, that there exists a change in circumstances sufficient to eliminate the need for the reporting requirement in Attachment D, and that the other provisions of this Agreement have been satisfied, the Agreement may be terminated early. If the Court refuses to grant an exclusion of time under the Speedy Trial Act, 18 U.S.C. § 3161(h)(2), the Term shall be deemed to have not begun and all the provisions of the

Agreement shall be deemed null and void, except that the statute of limitations for any prosecution relating to the conduct described in the Information and Statement of Facts shall be tolled from the date on which this Agreement was signed until the date the Court refuses to grant the exclusion of time, plus six months.

Relevant Considerations

4. The Office enters into this Agreement based on the individual facts and circumstances presented by this case and the Company, including:

a. the Company received partial credit for its cooperation with the Office's investigation of the underlying conduct, including collecting and producing evidence and voluntarily making employees, including senior employees, available for interviews in the United States;

b. the Company did not receive full credit for cooperation because the Company did not disclose relevant conduct set forth in the Statement of Facts until after it was identified in civil litigation;

c. the Company ultimately provided to the Office all relevant facts known to it, including information about the individuals involved in the misconduct;

d. the Company ultimately implemented remedial measures, including heightened controls and additional procedures and policies relating to the use and misuse of computer systems and passwords, and enhanced related training for all management and relevant employees;

e. the Company has committed to continuing to enhance its compliance program and internal controls, including ensuring that its compliance program satisfies the minimum elements set forth in Attachment C to this Agreement (Corporate Compliance Program);

f. based on the Company's remediation and the state of its compliance program, and the Company's agreement to report to the Office as set forth in Attachment D, the Office determined that an independent compliance monitor is unnecessary;

g. the nature and seriousness of the offense conduct, including, among other things, the duration of the scheme; the repeated instances of misconduct by at least one Company employee and one Company executive; the resulting benefits for the Company from the misconduct; and the commission of the misconduct in the presence of other Company employees; and

h. the Company has agreed to continue to cooperate with the Office's ongoing investigation, including as described in Paragraph 5 below.

i. Accordingly, after considering (a) through (h) above, the Office believes that the appropriate resolution in this case is a deferred prosecution agreement with the Company and a criminal monetary penalty of \$10,000,000, and the Company's agreement to report to the Office as set forth in Attachment D to this agreement.

Future Cooperation and Disclosure Requirements

5. The Company shall cooperate fully with the Office in any and all matters relating to the conduct described in this Agreement and the Statement of Facts, and other conduct under investigation by the Office at any time during the Term, subject to applicable laws and regulations, until the later of the date upon which all investigations and prosecutions arising out of such conduct

are concluded, or the end of the Term. At the request of the Office, the Company shall also cooperate fully with other domestic or foreign law enforcement and regulatory authorities and agencies in any investigation of the Company, its parents, branches, representative offices, subsidiaries or its affiliates, or any of its present or former officers, directors, employees, agents and consultants, or any other party, in any and all matters relating to the conduct described in this Agreement and the Statement of Facts. The Company's cooperation pursuant to this Paragraph is subject to applicable laws and regulations, including relevant data privacy and national security laws and regulations, as well as valid claims of attorney-client privilege or attorney work product doctrine; however, the Company must provide to the Office a log of any information or cooperation that is not provided based on an assertion of law, regulation or privilege, and the Company bears the burden of establishing the validity of any such assertion. The Company agrees that its cooperation pursuant to this Paragraph shall include, but not be limited to, the following:

a. The Company shall truthfully disclose all factual information with respect to its activities, those of its parents, branches, representative offices, subsidiaries and affiliates, and those of its present and former directors, officers, employees, agents and consultants, including any evidence or allegations and internal or external investigations, about which the Company has any knowledge and/or about which the Office may inquire. This obligation of truthful disclosure includes, but is not limited to, the obligation of the Company to provide to the Office, upon request, any document, record or other tangible evidence about which the Office may inquire of the Company.

b. Upon request of the Office, the Company shall designate knowledgeable employees, agents or attorneys to provide to the Office the information and materials described in

Paragraph 5(a) above on behalf of the Company. It is further understood that the Company must at all times provide complete, truthful and accurate information.

c. The Company shall use its best efforts to make available for interviews or testimony, as requested by the Office, present or former officers, directors, employees, agents and consultants of the Company. This obligation includes, but is not limited to, sworn testimony before a federal grand jury, in federal trials or at any other proceeding, all meetings requested by the Office, and interviews with domestic or foreign law enforcement and regulatory authorities. Cooperation under this Paragraph shall include identification of witnesses who, to the knowledge of the Company, may have material information regarding the matters being investigated or prosecuted.

d. With respect to any information, testimony, documents, records or other tangible evidence provided to the Office pursuant to this Agreement, the Company consents to any and all disclosures, subject to applicable laws and regulations, to other governmental authorities, including United States authorities and those of a foreign government of such materials as the Office, in its sole discretion, shall deem appropriate.

6. In addition to the obligations in Paragraph 5, during the Term, should the Company learn of any evidence or allegation of conduct that may constitute a violation of the CFAA or wire fraud statute that involve the employees or agents of the Company, the Company shall promptly report such evidence or allegation to the Office.

Payment of Monetary Penalty

7. The Office and the Company agree that, pursuant to Title 18, United States Code, Section 3571(c), an organization may be fined up to \$500,000 for each felony offense for which it has been found guilty.

8. The Office and the Company agree that employees of the Company engaged in at least twenty (20) discrete instances of unauthorized access of a protected computer in violation of the CFAA.

9. The Office and the Company agree that the Office could charge the Company with at least twenty (20) separate violations of Title 18, United States Code, Section 1030(a)(2) and/or Title 18, United States Code, Section 1030(a)(4).

10. The Office and the Company agree, based on the application of Title 18, United States Code, Section 3571(c), and the sentencing factors to be considered pursuant to Title 18, United States Code, Sections 3572 and 3553(a), that the total monetary penalty is \$10,000,000 (the "Total Criminal Penalty"). The Company and the Office further agree that the Total Criminal Penalty will be paid by the Company to the United States Treasury within ten business days of the execution of this Agreement.

11. The Company and the Office agree that the Total Criminal Penalty is appropriate given the facts and circumstances of this case. The Total Criminal Penalty is final and shall not be refunded. Furthermore, nothing in this Agreement shall be deemed an agreement by the Office that the Total Criminal Penalty is the maximum penalty that may be imposed in any future prosecution, and the Office is not precluded from arguing in any future prosecution that the Court should impose a higher fine, although the Office agrees that under those circumstances, it will

recommend to the Court that any amount paid under this Agreement should be offset against any fine the Court imposes as part of a future judgment. The Company acknowledges that no tax deduction may be sought in connection with the payment of any part of the Total Criminal Penalty. The Company shall not seek or accept directly or indirectly reimbursement or indemnification from any source with regard to the Total Criminal Penalty that the Company pays pursuant to this Agreement or any other agreement entered into with an enforcement authority or regulator concerning the facts set forth in the Statement of Facts.

Conditional Release from Liability

12. Subject to Paragraphs 18-21, the Office agrees, except as provided in this Agreement, that it will not bring any criminal or civil case against the Company or any of its parents, branches, representative offices or direct or indirect affiliates, subsidiaries or joint ventures based on the conduct described in the Statement of Facts and the Information filed pursuant to this Agreement. The Office, however, may use any information related to the conduct described in the Statement of Facts against the Company: (a) in a prosecution for perjury or obstruction of justice; (b) in a prosecution for making a false statement; (c) in a prosecution or other proceeding relating to any crime of violence; or (d) in a prosecution or other proceeding relating to a violation of any provision of Title 26 of the United States Code.

a. This Agreement does not provide any protection against prosecution for any other conduct by the Company or any of its parents, branches, representative offices or direct or indirect affiliates, subsidiaries or joint ventures.

b. In addition, this Agreement does not provide any protection against prosecution of any individuals, regardless of their affiliation with the Company.

Corporate Compliance Program

13. The Company represents that it has implemented and will maintain a compliance and ethics program designed to prevent and detect violations of the CFAA and other applicable laws, and to prevent the unauthorized and unlawful acquisition of confidential information belonging to its competitors (“competitor confidential information”) throughout its operations, including those of its parents and subsidiaries, and, where necessary and appropriate, its agents, joint ventures, and contractors, including, but not limited to, the minimum elements set forth in Attachment C.

14. In order to address any deficiencies in its internal controls, policies and procedures, the Company represents that it has undertaken, and will continue to undertake, in a manner consistent with all of its obligations under this Agreement, a review of its existing internal controls, policies and procedures regarding compliance with the CFAA and other applicable computer crime laws and prevention of the unauthorized and unlawful acquisition of competitor confidential information. Where necessary and appropriate, the Company agrees to modify or maintain its existing compliance program, including internal controls, compliance policies and procedures, in order to ensure that the program is effectively designed to maintain, prevent, detect and deter violations of the CFAA and other applicable computer crime laws, or the unauthorized and unlawful acquisition of confidential information belonging to the Company’s competitors. The compliance program will include, but not be limited to, the minimum elements set forth in Attachment C.

Corporate Compliance Reporting

15. The Company agrees that it will report to the Office annually during the Term regarding remediation and implementation of the compliance measures described in Attachment C. These reports will be prepared in accordance with Attachment D.

Deferred Prosecution

16. In consideration of the undertakings agreed to by the Company herein, the Office agrees that any prosecution of the Company for the conduct set forth in the Statement of Facts be, and hereby is, deferred for the Term. To the extent there is conduct disclosed by the Company that is not set forth in the Statement of Facts, such conduct will not be exempt from further prosecution and is not within the scope of or relevant to this Agreement.

17. The Office further agrees that if the Company fully complies with all of its obligations under this Agreement, the Office will not continue the criminal prosecution against the Company described in Paragraph 1 and, at the conclusion of the Term, this Agreement shall expire. Within six months of the Agreement's expiration, the Office shall seek dismissal with prejudice of the criminal Information filed against the Company described in Paragraph 1, and agree not to file charges in the future against the Company based on the conduct described in the Statement of Facts and Information. If, however, the Office determines during this six-month period that the Company breached the Agreement during the Term, as described in Paragraph 18, the Office's ability to extend the Term, as described in Paragraph 3, or to pursue other remedies, including those described in Paragraphs 18-21, remains in full effect.

Breach of the Agreement

18. If, during the Term, the Company (a) commits any felony under U.S. federal law; (b) provides in connection with this Agreement deliberately false, incomplete or misleading

information, including in connection with its disclosure of information about individual culpability; (c) fails to cooperate as set forth in Paragraphs 5 and 6 of this Agreement; (d) fails to implement or maintain a compliance program as set forth in Paragraphs 13 and 14 of this Agreement and Attachment C; or (e) otherwise fails to completely perform or fulfill its obligations under the Agreement, regardless of when the Office becomes aware of such a breach, the Company shall thereafter be subject to prosecution for any federal criminal violation of which the Office has knowledge, including, but not limited to, the charges in the Information described in Paragraph 1, which may be pursued by the Office in the U.S. District Court for the Eastern District of New York or any other appropriate venue. Determination of whether the Company has breached the Agreement and whether to pursue prosecution of the Company shall be in the Office's sole discretion. Any such prosecution may be premised on information provided by the Company or its personnel. Any such prosecution relating to the conduct described in the Statement of Facts or relating to conduct known to the Office prior to the date on which this Agreement was signed that is not time-barred by the applicable statute of limitations on the date of the signing of this Agreement may be commenced against the Company, notwithstanding the expiration of the statute of limitations, between the signing of this Agreement and the expiration of the Term plus one year. Thus, by signing this Agreement, the Company agrees that the statute of limitations with respect to any such prosecution that is not time-barred on the date of the signing of this Agreement shall be tolled for the Term plus one year. In addition, the Company agrees that the statute of limitations as to any violation of federal law that occurs during the Term will be tolled from the date upon which the violation occurs until the earlier of the date upon which the Office is made aware of the

violation or the duration of the Term plus five years, and that this period shall be excluded from any calculation of time for purposes of the application of the statute of limitations.

19. In the event the Office determines that the Company has breached this Agreement, the Office agrees to provide the Company with written notice of such breach prior to instituting any prosecution resulting from such breach. Within thirty days of receipt of such notice, the Company shall have the opportunity to respond to the Office in writing to explain the nature and circumstances of such breach, as well as the actions the Company has taken to address and remediate the situation, which explanation the Office shall consider in determining whether to pursue prosecution of the Company.

20. In the event that the Office determines that the Company has breached this Agreement: (a) all statements made by or on behalf of the Company to the Office and to the Court, including the Statement of Facts, and any testimony given by the Company before a grand jury, a court or any tribunal, or at any legislative hearings, whether prior or subsequent to entering this Agreement, and any leads derived from such statements or testimony, shall be admissible in evidence in any and all criminal proceedings brought by the Office against the Company; and (b) the Company shall not assert any claim under the United States Constitution, Rule 11(f) of the Federal Rules of Criminal Procedure, Rule 410 of the Federal Rules of Evidence or any other federal rule that any such statements or testimony made by or on behalf of the Company prior or subsequent to this Agreement, or any leads derived therefrom, should be suppressed or are otherwise inadmissible. The decision as to whether any conduct or statements of any director, officer or employee, or any person acting on behalf of, or at the direction of, the Company, will be

imputed to the Company for the purpose of determining whether the Company has violated any provision of this Agreement shall be in the sole discretion of the Office.

21. The Company acknowledges that the Office has made no representations, assurances or promises concerning what sentence may be imposed by the Court if the Company breaches this Agreement and this matter proceeds to judgment. The Company further acknowledges that any such sentence is solely within the discretion of the Court and that nothing in this Agreement binds or restricts the Court in the exercise of such discretion.

22. On the date that the period of deferred prosecution specified in this Agreement expires, the Company, by the President of the Company and the Chief Compliance Officer of the Company, will certify, in the form of executing the document attached as Attachment E to this Agreement, to the Office that the Company has met its disclosure obligations pursuant to Paragraph 6 of this Agreement. Each certification will be deemed a material statement and representation by the Company to the executive branch of the United States for purposes of 18 U.S.C. §§ 1001 and 1519, and it will be deemed to have been made in the Eastern District of New York.

Sale, Merger or Other Change in Corporate Form of Company

23. Except as may otherwise be agreed by the parties in connection with a particular transaction, the Company agrees that in the event that, during the Term, it undertakes any change in corporate form, including if it sells, merges or transfers business operations that are material to the Company's consolidated operations, or to the operations of any parents, branches, representative offices, subsidiaries or affiliates involved in the conduct described in the Statement of Facts, as they exist as of the date of this Agreement, whether such sale is structured as a sale,

asset sale, merger, transfer or other change in corporate form, it shall include in any contract for sale, merger, transfer or other change in corporate form a provision binding the purchaser, or any successor in interest thereto, to the obligations described in this Agreement. The purchaser or successor in interest must also agree in writing that the Office's ability to declare a breach under this Agreement is applicable in full force to that entity. The Company agrees that a failure to include these provisions in the transaction will make any such transaction null and void. The Company shall provide notice to the Office at least thirty days prior to undertaking any such sale, merger, transfer or other change in corporate form. The Office shall notify the Company prior to such transaction (or series of transactions) if it determines that the transaction(s) will have the effect of circumventing or frustrating the enforcement purposes of this Agreement. At any time during the Term, if the Company engages in a transaction that has the effect of circumventing or frustrating the enforcement purposes of this Agreement, the Office may deem it a breach of this Agreement pursuant to Paragraphs 18-21 of this Agreement. Nothing herein shall restrict the Company from indemnifying or otherwise holding harmless the purchaser or successor in interest for penalties or other costs arising from any conduct that may have occurred prior to the date of the transaction, provided that such indemnification does not have the effect of circumventing or frustrating the enforcement purposes of this Agreement, as determined by the Office.

Public Statements by Company

24. The Company expressly agrees that it shall not, through present or future attorneys, officers, directors, employees, agents or any other person authorized to speak for the Company, make any public statement, in litigation or otherwise, contradicting the acceptance of responsibility by the Company set forth above or the facts described in the Statement of Facts. Any such

contradictory statement shall, subject to cure rights of the Company described below, constitute a breach of this Agreement, and the Company thereafter shall be subject to prosecution as set forth in Paragraphs 18-21 of this Agreement. The decision as to whether any public statement by any such person contradicting a fact contained in the Statement of Facts will be imputed to the Company for the purpose of determining whether it has breached this Agreement shall be at the sole discretion of the Office. If the Office determines that a public statement by any such person contradicts in whole or in part a statement contained in the Statement of Facts, the Office shall so notify the Company, and the Company may avoid a breach of this Agreement by publicly repudiating such statement within five business days after notification. The Company shall be permitted to raise defenses and to assert affirmative claims in other proceedings relating to the matters set forth in the Statement of Facts provided that such defenses and claims do not contradict, in whole or in part, a statement contained in the Statement of Facts. This Paragraph does not apply to any statement made by any present or former officer, director, employee or agent of the Company in the course of any criminal, regulatory or civil case initiated against such individual, unless such individual is speaking on behalf of the Company.

25. The Company agrees that if it or any of its parents, branches, representatives or direct or indirect subsidiaries, affiliates or joint ventures issues a press release or holds any press conference in connection with this Agreement, the Company shall first consult with the Office to determine (a) whether the text of the release or proposed statements at the press conference is true and accurate with respect to matters between the Office and the Company; and (b) whether the Office has any objection to the release or statement.

26. The Office agrees, if requested to do so, to bring to the attention of law enforcement and regulatory authorities the facts and circumstances relating to the nature of the conduct underlying this Agreement, including the nature and quality of the Company's cooperation and remediation. By agreeing to provide this information to such authorities, the Office is not agreeing to advocate on behalf of the Company, but rather is agreeing to provide facts to be evaluated independently by such authorities. Nothing in this Agreement restricts in any way the ability of the Office, any other federal department or agency, or any state or local government from proceeding criminally, civilly or administratively against any current or former directors, officers, employees or agents of the Company or against any other entities or individuals. The parties to this Agreement intend that the Agreement does not confer or provide any benefits, privileges, immunities or rights to any other individual or entity other than the parties hereto.

Limitations on Binding Effect of Agreement

27. This Agreement is binding on the Company and the Office but does not bind any other component of the Department of Justice, any other federal agency, or any state, local or foreign law enforcement or regulatory agency, or any other authority, although the Office will bring the cooperation of the Company and its compliance with its other obligations under this Agreement to the attention of such agencies and authorities if requested to do so by the Company.

Notice

28. Any notice to the Office under this Agreement shall be given by electronic mail ("e-mail") and personal delivery, overnight delivery by a recognized delivery service, or registered or certified mail, addressed to Chief, National Security and Cybercrime Section, U.S. Attorney's Office for the Eastern District of New York, 271-A Cadman Plaza East, Brooklyn, New York,

11201. Any notice to the Company under this Agreement shall be given by e-mail or personal delivery, overnight delivery by a recognized delivery service, or registered or certified mail, addressed to (a) Michael Rowles, General Counsel for the Company, at MichaelRowles@livenation.com and (b) Serrin Turner of Latham & Watkins LLP, at Serrin.Turner@lw.com. Notice shall be effective upon actual receipt by the Office or the Company.


Complete Agreement

29. This Agreement, including its attachments, sets forth all the terms of the agreement between the Company and the Office. No amendments, modifications or additions

to this Agreement shall be valid unless they are in writing and signed by the Office, the attorneys for the Company, and a duly authorized representative of the Company.


**AGREED:
FOR TICKETMASTER L.L.C.**

Date: 12/29/2020

By: 

Michael Rowles
General Counsel
Ticketmaster L.L.C.

Date: 12/29/2020

By: 

Serrin Turner
Latham & Watkins, LLP

FOR THE UNITED STATES ATTORNEY'S OFFICE

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

Date: 12/29/2020

By: 

Allon Lifshitz
Craig R. Heeren
Ian C. Richardson
Assistant United States Attorneys


COMPANY OFFICER’S CERTIFICATE

I have read this Agreement and carefully reviewed every part of it with outside counsel for Ticketmaster L.L.C. (the “Company”). I understand the terms of this Agreement and voluntarily agree, on behalf of the Company, to each of its terms. Before signing this Agreement, I consulted outside counsel for the Company. Counsel fully advised me of the rights of the Company, of possible defenses, of the Sentencing Guidelines’ provisions, and of the consequences of entering into this Agreement.

I have carefully reviewed the terms of this Agreement with the Board of Directors and the Company’s Chief Compliance Officer. I have advised the Board of Directors and the Chief Compliance Officer fully of the rights of the Company, of possible defenses, of the Sentencing Guidelines’ provisions, and of the consequences of entering into the Agreement.

No promises or inducements have been made other than those contained in this Agreement. Furthermore, no one has threatened or forced me, or, to my knowledge, any person authorizing this Agreement on behalf of the Company, in any way to enter into this Agreement. I am also satisfied with outside counsel’s representation in this matter. I certify that I am the General Counsel for the Company, and that I have been duly authorized by the Company to execute this Agreement on behalf of the Company.

Date: 12/29/2020

By: 

Michael Rowles
General Counsel
Ticketmaster L.L.C.

CERTIFICATE OF COUNSEL

I am counsel for Ticketmaster L.L.C. (the “Company”) in the matter covered by this Agreement. In connection with such representation, I have examined relevant Company documents and have discussed the terms of this Agreement with the General Counsel of the Company. Based on our review of the foregoing materials and discussions, I am of the opinion that the representative of the Company has been duly authorized to enter into this Agreement on behalf of the Company and that this Agreement has been duly and validly authorized, executed and delivered on behalf of the Company and is a valid and binding obligation of the Company. Further, I have carefully reviewed the terms of this Agreement with the General Counsel of the Company. I have fully advised him of the rights of the Company, of possible defenses, of the Sentencing Guidelines provisions and of the consequences of entering into this Agreement. To my knowledge, the decision of the Company to enter into this Agreement, based on the authorization of the Board of Directors, is an informed and voluntary one.

Date: 12/29/2020

By: _____

Serrin Turner
Latham & Watkins LLP

ATTACHMENT A
STATEMENT OF FACTS

The following Statement of Facts is incorporated by reference as part of the Deferred Prosecution Agreement (the “Agreement”) between the United States Attorney’s Office for the Eastern District of New York (the “Office”) and the defendant, Ticketmaster L.L.C. (the “Company”). The Company hereby agrees and stipulates that the following facts are true and accurate. Certain of the facts herein are based on information obtained from third parties by the United States through its investigation and described to the Company. The Company admits, accepts and acknowledges that it is responsible for the acts of its officers, directors, employees and agents as set forth below. Should the United States pursue the prosecution that is deferred by this Agreement, the Company agrees that it will neither contest the admissibility of, nor contradict, this Statement of Facts in any such proceeding. The following facts took place in or about and between August 2013 and December 2015, unless otherwise noted.

At all times relevant to this Statement of Facts:

I. The Defendant, Victim Company and Relevant Participants

1. The defendant TICKETMASTER L.L.C. (“TICKETMASTER”), is and was at all relevant times a wholly owned subsidiary of Live Nation Entertainment, Inc. (“Live Nation”), a publicly traded corporation that operated from offices located in New York, New York; San Francisco and Los Angeles, California; and other locations. TICKETMASTER is and was primarily engaged in the business of selling and distributing tickets to events and concerts at venues with which it had contracted to host such events and concerts.

2. The Victim Company¹ was a company based in the United Kingdom, with U.S. headquarters in Brooklyn, New York, that sold presale tickets, described in greater detail below, for musical artists and management companies. The Victim Company merged with another company in or about 2015, and declared bankruptcy in 2016.

3. Coconspirator-1 was a citizen of the United Kingdom who resided in Brooklyn, New York. Coconspirator-1 was the Victim Company's first employee in the United States and worked in the Victim Company's offices in Brooklyn, first as a consultant in March 2010, and then as the Senior Vice President for Global Operations and General Manager for North America from approximately May 2010 to July 26, 2012. Coconspirator-1 became employed by Live Nation in its TicketWeb subsidiary in approximately August 2013. In approximately January 2015, he was promoted to Director of Client Relations in TICKETMASTER's Artist Services division and received a raise. Coconspirator-1 was terminated by Live Nation and TICKETMASTER in approximately October 2017.

4. Zeeshan Zaidi was a citizen of Canada and a naturalized citizen of the United States, with graduate degrees from Harvard Law School and Harvard Business School, who resided in New York, New York. In approximately November 2013, Zaidi was retained by Live Nation as a consultant to work on a project, as to which he reported to senior executives of TICKETMASTER. In approximately August 2014, Zaidi was formally hired to lead TICKETMASTER's Artist Services division. In approximately October 2017, Zaidi was terminated by Live Nation and TICKETMASTER. On October 18, 2019, Zaidi pled guilty in the

¹ The identities of the Victim Company and all other individuals and entities referred to in this Statement of Facts are known to the United States Attorney.

United States District Court for the Eastern District of New York to one count of conspiring to access protected computers without authorization and to commit wire fraud, in violation of Title 18, United States Code, Section 371. See United States v. Zeeshan Zaidi, 19 CR 450 (MKB) (E.D.N.Y.).

II. Factual Background

5. As detailed below, TICKETMASTER employees and agents, including Coconspirator-1 and Zaidi, accessed Victim Company computer systems without authorization from Live Nation and TICKETMASTER computer systems on numerous occasions between August 2013 and December 2015. The information obtained from such unauthorized access was used for, among other things, preparing strategy presentations for senior Live Nation and TICKETMASTER executives that benchmarked competitor products and services, including those offered by the Victim Company.

A. The Presale Ticketing Market

6. Through a corporate division known during the relevant time period as “Artist Services,” TICKETMASTER sold “presale tickets,” which were tickets to an event that were sold in advance of general ticket sales, typically through an artist’s website to members of a “fan club” or through some other promotion. Although TICKETMASTER’s contracts with venues gave it exclusive rights to sell all tickets at particular events, TICKETMASTER allowed artists to sell a portion of presale tickets “off platform,” i.e., on their own or through another company. Typically, TICKETMASTER permitted up to 8% of presale tickets to be sold off-platform by another company, provided that certain rules established by TICKETMASTER were followed. Off-platform sales reflected a loss of revenue to TICKETMASTER, because TICKETMASTER

was unable to charge service fees in connection with the sale of off-platform tickets. One of the business responsibilities of TICKETMASTER's Artist Services division was to encourage artists and their management companies to use TICKETMASTER's ticketing platform to sell presale tickets, and in certain circumstances to discourage artists from using competitor ticketing services to sell presale tickets off-platform.

7. The Victim Company offered artists the ability to sell presale tickets off of TICKETMASTER's platform by operating or helping the artist to operate an online ticketing platform. As part of its services to its artist clients, the Victim Company offered a data analytics package for ticketing known as an Artist Toolbox (the "Toolbox"). The Toolbox was a web-based software application that provided the artists or the artist's manager real-time data about ticket sales effected through the Victim Company. Among other things, the Toolbox provided information about where tickets were being purchased, the number of tickets sold at each venue, information about tickets sold on particular dates and email addresses collected from ticket purchasers that could then be added to artists' mailing lists. The Toolbox was designed for use by the artist and his or her management company. Toolboxes were generally set up for each artist or manager who did business with the Victim Company, and each Toolbox was protected with a unique username and password known to the artist and/or manager, as well as Victim Company employees.

8. The Victim Company created individualized web pages for its clients showing event listings and containing "Buy Tickets" links that users could use to purchase tickets. The Victim Company also created such web pages for artists in draft form. These draft ticketing web pages were either "mock" sites used to market the Victim Company's services to prospective

clients, or dormant because the event had not yet been announced. The Victim Company's draft ticketing web pages were accessible via the Internet and were not password-protected. However, the web pages were not indexed in search engines, and therefore could not be located by the public using search engines such as Google. Instead, in order to access one of the ticketing web pages, a person would have to figure out its exact Uniform Resource Locator ("URL"), *i.e.*, its webpage address. The Victim Company did not advertise these webpages to the public until the artist and its management company were ready to sell tickets to the artist's shows. Until the Victim Company, the artist or the artist's manager publicly disseminated the URLs to the ticketing web pages, the Victim Company intended to restrict access to the ticketing web pages only to the Victim Company, the artist and the artist management company.

B. Coconspirator-1's Separation Agreement and Employment by Live Nation and TICKETMASTER

9. During and in the course of his employment with the Victim Company, Coconspirator-1 was given access to confidential and proprietary information about the Victim Company and its clients, including the usernames and passwords to the Victim Company Toolboxes, and the Victim Company's practice of creating draft ticketing web pages for clients or prospective clients, thus allowing him to locate URL addresses for such pages even after he left the Victim Company in 2012.

10. On or about August 28, 2012, Coconspirator-1 signed a "Separation and Release Agreement" with the Victim Company (the "Separation Agreement"). Under the Separation Agreement, Coconspirator-1 acknowledged that during his employment he "had access to confidential and proprietary information relating to [the Victim Company], its artists, its business and third parties with whom [the Victim Company] does or did business." The Separation

Agreement listed illustrative examples of the types of confidential information to which Coconspirator-1 had access, including “client lists,” “passwords,” “marketing strategies” and “financial information.” Under the terms of the Separation Agreement, Coconspirator-1 agreed that “[a]t all times hereafter,” he would “maintain the confidentiality of all Confidential Information,” and that he would not “directly or indirectly, make any disclosure of Confidential Information to any third party” or “make any use of Confidential Information” for Coconspirator-1’s “own benefit or the benefit of any third party, without [the Victim Company’s] prior written consent.”

11. Coconspirator-1 further agreed that he would return to the Victim Company “all material or documents containing Confidential Information” and would “not retain any copies, duplicates, reproductions or excerpts of such material or documents.” Coconspirator-1 agreed that until July 26, 2013, he would not “engage in the businesses of direct retail ticketing, presale ticketing or technology ticketing enablement services,” and would not “accept employment, consult for or participate, directly or indirectly, in the ownership or management of any enterprise anywhere in the United States engaged in such a business.”

12. In exchange for agreeing to these and other terms, and as part of this Separation Agreement, the Victim Company paid Coconspirator-1 approximately \$52,970.

13. In or about May 2013, Coconspirator-1 sent an email attaching his resume to a Vice President of TICKETMASTER who worked in its Artist Services division (“Executive-1”). Executive-1 then emailed Coconspirator-1’s resume to a Live Nation executive at a different division of the company called TicketWeb that focused on ticketing at small venues (“Executive-2”), and noted Coconspirator-1’s “ticketing experience that includes a stint at [Victim

Company].” Coconspirator-1 subsequently spoke with another Live Nation TicketWeb executive about a position in client development (“Executive-3”). On or about May 28, 2013, Coconspirator-1 completed an application for employment with Live Nation.

14. In or about June 2013, Coconspirator-1 discussed the Separation Agreement with Executive-3 and emailed him a copy of the Separation Agreement. On or about July 1, 2013, Live Nation offered Coconspirator-1 a client development position at TicketWeb in a written letter (the “Offer Letter”).

15. The Offer Letter specifically referenced Coconspirator-1’s Separation Agreement and “remind[ed]” Coconspirator-1 of his “obligations to preserve the trade secrets and confidential and proprietary information of [Coconspirator-1’s] current and prior employers.” The Offer Letter further advised Coconspirator-1 that he “must not retain copies of any trade secret or confidential and proprietary information of any prior employer,” and further warned Coconspirator-1 that he could “not bring such materials to work or otherwise utilize such materials as part of [his] work for [Live Nation].” In signing the letter and accepting the offer, Coconspirator-1 agreed that he had “not taken any trade secret or confidential or proprietary information from [his] former employers and ha[d] not disclosed any such information to any employees of Live Nation Entertainment.” Coconspirator-1 further acknowledged his “obligation not to disclose any such information in the future.”

16. On or about July 2, 2013, Coconspirator-1 signed the Offer Letter and accepted Live Nation’s offer of employment.

17. On or about August 2, 2013, shortly after beginning his employment with Live Nation at TicketWeb, Coconspirator-1 signed Live Nation’s standard “Proprietary

Information Agreement,” in which he agreed to maintain the confidentiality of, and not to disclose, confidential proprietary information owned by Live Nation. Live Nation’s Proprietary Information Agreement contained the following paragraph:

I understand that [Live Nation] does not want, and will not permit me to access, use, or disclose, any confidential or proprietary information belonging to any third parties, including former employers. I represent and warrant and covenant that I have not and will not disclose to [Live Nation], or use in connection with my activities as an employee of [Live Nation], or induce [Live Nation] to use, any proprietary or confidential information or trade secrets, or any other subject matter that is the subject of Proprietary Rights, of myself or any third party at any time, including, without limitation, any proprietary or confidential information or trade secrets of any former employer.

III. TICKETMASTER Solicits and Obtains Victim Company Information from Coconspirator-1

18. From the beginning of Coconspirator-1’s employment with Live Nation, he repeatedly violated his duty to protect the Victim Company’s confidential and proprietary information, as set forth in Live Nation’s own internal policies and agreements with Coconspirator-1 and in Coconspirator-1’s Separation Agreement with the Victim Company. Among other things, Coconspirator-1 and TICKETMASTER executives accessed, without authorization, protected Victim Company computer systems in order to obtain Victim Company information. They did so using log-in credentials that Coconspirator-1 had obtained during his employment with the Victim Company and retained in violation of the Separation Agreement and Live Nation policy. TICKETMASTER executives, including Zaidi, also solicited, and Coconspirator-1 provided, confidential proprietary information about the Victim Company and its business that Coconspirator-1 had obtained while employed by the Victim Company.

A. TICKETMASTER Executives Solicit Victim Company Information from Coconspirator-1

19. Just weeks after Coconspirator-1 started working at TicketWeb, TICKETMASTER executives began soliciting information from Coconspirator-1 regarding the Victim Company.

20. For example, on or about August 29, 2013, Executive-2 emailed Coconspirator-1 a draft presentation intended for a high-level corporate officer of Live Nation (“Corporate Officer-1”) and a high-level corporate officer of TICKETMASTER (“Corporate Officer-2”) that analyzed TICKETMASTER’s competitors in the presale ticketing market, and asked Coconspirator-1 for his insight about “the competitive gaps with some of the smaller providers.” Coconspirator-1 responded with a detailed analysis of the Victim Company’s competitive strengths relative to TICKETMASTER, which Executive-2 used to update the presentation and emailed to, among others, Executive-1.

21. In or about November 2013, Executive-2 again asked Coconspirator-1 to provide information regarding Coconspirator-1’s former employer, this time to TICKETMASTER executive Zaidi, described as “a new member of the Ticketmaster team” who had joined TICKETMASTER to “formulate a compelling offer for Artist (presales, merch, fanclubs, etc).” Coconspirator-1 agreed, promising Executive-2 and Zaidi that he would “pass on as much information as you need about [the Victim Company].”

22. In subsequent emails in or about November 2013, regarding a new tour planned by an artist that Coconspirator-1 described as “a financial foundation for [the Victim Company] from day one,” Coconspirator-1 offered to provide Executive-2 and Zaidi information regarding the fees applied by the Victim Company to ticket prices, and Coconspirator-1 shared

with them the URLs for draft ticketing web pages that the Victim Company had built for the artist's planned and previous tours but had not disseminated to the public. Coconspirator-1 made clear that he obtained the information because, while employed at the Victim Company, he had personally handled the artist's tours in North and South America. During these communications, Executive-2 described how the goal was to "choke off [Victim Company]" and "steal back one of [Victim Company]'s signature clients." Coconspirator-1 responded by offering that they could "cut [Victim Company] off at the knees" if they could win back presale ticketing business for a second major artist by offering the same ticketing fee structure that the Victim Company gave to the second artist.

B. January to June 2014: Coconspirator-1 and Other TICKETMASTER Executives Repeatedly Access the Victim Company Computer Systems Without Authorization

23. On or about January 9, 2014, Coconspirator-1 emailed Executive-1 and Zaidi a collection of "info from [the Victim Company] that might be useful as an insight into their operations."

24. The first category of information Coconspirator-1 provided included usernames and passwords for Toolboxes that the Victim Company had established for three different artist management companies. Coconspirator-1 encouraged the two TICKETMASTER executives to "screen-grab the hell out of the system," and warned them that Coconspirator-1 and TICKETMASTER were not authorized to access the Victim Company Toolboxes:

I must stress that as this is access to a live [Victim Company] tool I would be careful in what you click on as it would be best not [to] giveaway that we are snooping around.

(Emphasis in original.) In addition, Coconspirator-1 attached two Victim Company-related Excel spreadsheets: (1) a “booking fee calculator” that gave “the full breakdown of the fees [the Victim Company] appl[ies] to the . . . normal ticket prices”; and (2) an “Account Management Tool” that “was used for every new artist tour” to “provide the biz-dev and client services guys an idea of the profitability of the tour.”

25. Zaidi responded to Coconspirator-1’s email with approval: “Awesome – thanks [Coconspirator-1]!”

26. Later the same day, Coconspirator-1, Executive-1 and Zaidi participated in a conference call, during which Coconspirator-1 used, without authorization, the Victim Company’s usernames and passwords to access Victim Company Toolboxes, and used Internet presentation software to demonstrate the functionality of the Victim Company Toolbox application and data to Executive-1 and Zaidi. Coconspirator-1 and Zaidi participated in this call from TICKETMASTER’s New York office, and Executive-1 participated from TICKETMASTER’s Los Angeles office.

27. Zaidi promptly made use of the information to prepare a presentation for other senior TICKETMASTER executives that was intended to “benchmark,” or compare, TICKETMASTER’s Artist Services and other ticket offerings against those of, among other competitors, the Victim Company. Included in the presentation, which Zaidi emailed on or about January 10, 2014, were multiple slides that included screenshots of the Victim Company Toolboxes that were accessed the previous day by Coconspirator-1, Executive-1 and Zaidi.

28. In or about May 2014, Corporate Officer-1 and Corporate Officer-2, communicated several questions about the Victim Company to Zaidi. Subsequently, Zaidi,

Coconspirator-1 and other TICKETMASTER employees made additional unauthorized intrusions into protected Victim Company computer systems to collect information about the Victim Company's presale offerings to artists.

29. On or about May 8, 2014, Corporate Officer-1 emailed, among others, Corporate Officer-2, Executive-1 and Zaidi, stating "[Victim Company] pushing hard – I need to see exact plan for our fan club product when we announce it etc[.]" After Zaidi responded with some general information about timing, Corporate Officer-1 clarified that his focus was on understanding how TICKETMASTER's presale online offering compared with the Victim Company's Toolbox: "When can you show me wireframes etc so I can see exact [Victim Company] vs our product[?]"

30. Zaidi turned to Coconspirator-1 for help responding to this request from Live Nation's senior management. On or about May 11, 2014, Zaidi emailed Coconspirator-1, explaining that "[o]n the [Victim Company] front, I'm now preparing a deck for [Corporate Officer-1] about our strategy, especially to create comparable platforms," and asked if Coconspirator-1 could "do a screenshare/demo" on May 14, 2014, at a meeting in San Francisco, California with employees from TICKETMASTER's Artist Services division who had been tasked with "building the platform."

31. Coconspirator-1 responded that he would "be happy to help out," and Zaidi replied that he wanted Coconspirator-1 to demonstrate the Victim Company's Toolbox. Coconspirator-1 specifically told Zaidi that he would "pull together a list of the log-ins and URL's that I still have access to for this so I can give the team as much insight as possible." Zaidi responded, "That would be perfect."

32. On or about May 12, 2014, Zaidi emailed multiple TICKETMASTER employees in the Artist Services division with an agenda for a two-day Artist Services “Summit” meeting in San Francisco beginning on or about May 14, 2014. The second item on the agenda for that day was “[Victim Company]: product review (1.5 hrs).” Zaidi further noted, “[Coconspirator-1] will be coming in for this!”

33. At least 14 Live Nation and TICKETMASTER employees were in attendance at the Artist Services Summit on or about May 14, 2014, including, among others, Coconspirator-1, Executive-1, Executive-2 and Zaidi. During his presentation, Coconspirator-1 used a username and password he had retained from his employment at the Victim Company to log in to a Victim Company Toolbox, without authorization, from a Live Nation computer. Coconspirator-1 provided a demonstration of the Toolbox application and the data that the Victim Company made available to its clients. Coconspirator-1 projected his presentation onto a large screen in a conference room for the benefit of the participants of the meeting.

34. Log data obtained from the Victim Company indicates that on or about May 14, 2014, between 10:43 a.m. and 11:14 a.m. Pacific Time, the approximate time of Coconspirator-1’s presentation, an individual or individuals logged into a Victim Company Toolbox for a specific artist management company from an Internet Protocol (“IP”) address registered to a subsidiary of Live Nation based in San Francisco, California.

35. On or about May 27, 2014, following the Artist Services Summit, Zaidi emailed a draft presentation intended for Corporate Officer-1 to other employees in the Artist Services division. The presentation evaluated the strengths and weaknesses of competitors’ product offerings and included screenshots from some of the Victim Company Toolboxes that had

been accessed in or about January 2014 by Coconspirator-1, Executive-1 and Zaidi. In his email, Zaidi asked the Artist Services division employees to assist him with refining the presentation, and they turned to Coconspirator-1 for more information about the Victim Company.

36. For example, on or about May 28, 2014, a TICKETMASTER marketing executive (“Executive-4”) asked Coconspirator-1 to help Executive-4 estimate the Victim Company’s annual business so that the presentation could articulate to Corporate Officer-1 “what is on the table for us to try and win back with our new service offering[.]” The following day, Coconspirator-1 responded to Executive-4 and, copying Zaidi, provided an internal Victim Company “Weekly Heads of Department” report that Coconspirator-1 had retained from his employment with the Victim Company, explaining that it “included the projections vs real sales across tickets and merch in all territories that [the Victim Company] operated in.” Coconspirator-1 also provided “[the Victim Company’s] Growth plan for 2012/2013,” which he had retained from his employment at the Victim Company, stating that he had already provided it to Zaidi “at the beginning of the year.” Coconspirator-1 stated that he hoped the attached documents would provide Executive-4 with “insight in the [Victim Company] business.”

37. On or about June 2, 2014, Coconspirator-1 again emailed Zaidi the Victim Company Toolbox usernames and passwords that he had sent in or about January 2014, and included three new sets of Toolbox usernames and passwords. Coconspirator-1 again repeated the same warning that access to the Victim Company Toolboxes was unauthorized:

I must stress that as this is access to a live [Victim Company] tool I would be careful in what you click on as it would be best not [to] giveaway that we are snooping around.

(Emphasis in original.) Log data obtained from the Victim Company indicates that the three new Victim Company Toolboxes identified in Coconspirator-1's email were accessed from an IP address registered to TICKETMASTER's New York offices on or about June 2, 2014.

38. On or about June 3, 2014, Zaidi reviewed the presentation with Corporate Officer-2.

39. On or about June 19, 2014, Zaidi emailed a revised version of the presentation to Corporate Officer-1, Corporate Officer-2 and another high-level corporate officer of Live Nation ("Corporate Officer-3"). The presentation again included the screenshots of the Victim Company Toolbox taken in or about January 2014.

40. After giving the presentation to Corporate Officer-1, Corporate Officer-2 and Corporate Officer-3, Zaidi distributed slides from the presentation, including those containing screenshots of the Victim Company Toolbox, to a senior Live Nation executive ("Executive-5") on or about August 28, 2014. Zaidi asked Executive-5 to maintain the confidentiality of the slides because they provided "a look into the [the Victim Company] platform."

41. In or about August 2014, Corporate Officer-2 promoted Zaidi to head of TICKETMASTER's Artist Services division. In or about January 2015, Coconspirator-1 was transferred from TicketWeb, promoted to Director of Client Relations in TICKETMASTER's Artist Services division, and given a raise. Coconspirator-1 worked directly for Zaidi in Artist Services. Following the announcement of his promotion, on or about January 13, 2015, Coconspirator-1 emailed another TICKETMASTER Artist Services employee: "It's great to be part of the Artist Services team! Now we can really start to bring down the hammer on [Victim Company]."

C. July 2014-June 2015: TICKETMASTER's Continued Surveillance of the Victim Company and Intrusions Into Its Computer Systems

42. As detailed above, the Victim Company created ticketing web pages in advance of its artist clients' tours, often before it was public knowledge that the artist had decided to use the Victim Company instead of TICKETMASTER to sell tickets. Although the web pages were not password-protected, they were not indexed in search engines, and therefore could not be located or accessed without figuring out the exact URL for the ticketing web page, which included a series of numbers.

43. After joining Live Nation, Coconspirator-1 explained to Zaidi and others how the "store ID" numbers in the URLs for the Victim Company's ticketing web pages were numbered sequentially, enabling TICKETMASTER employees to browse through them to find and monitor new ticketing web pages to learn which artists planned to use the Victim Company to sell tickets for their shows. Coconspirator-1 used this information periodically to search for new Victim Company ticketing web pages, and sent the URLs to TICKETMASTER executives to provide intelligence about the Victim Company's business and artist clients.

44. For example, on or about July 14, 2014, Coconspirator-1 sent an email to Executive-1, Zaidi and another TICKETMASTER executive ("Executive-6") identifying 12 URLs for Victim Company ticketing web pages that had not been publicly disseminated, in order to make the executives aware of "what the scallywags over at [the Victim Company] are working on." Coconspirator-1 followed this email on or about July 22, 2014, with an email to the same TICKETMASTER executives with two new URLs to Victim Company ticketing web pages, writing, "More new [Victim Company] activity for you." On or about July 29, 2014, Coconspirator-1 sent another email with four new URLs to Victim Company ticketing web pages

to the same TICKETMASTER executives, writing “Today’s [Victim Company] client update,” and followed with an assessment stating: “[Victim Company] are having a higher success rate as seen in the amount of test sites being updated to a live pre-sale campaigns as of late.” Coconspirator-1 then asked the TICKETMASTER executives whether there had been any progress determining “what we can offer to deter these artists/managers from using [Victim Company] services?”

45. In or about January 2015, Zaidi assigned a TICKETMASTER employee based in Los Angeles, California to learn what he called the Victim Company’s “link numbering system” from Coconspirator-1 so that the employee could actively search for and monitor the ticketing web pages created by the Victim Company for competitive intelligence. That employee maintained a spreadsheet listing every Victim Company ticketing web page that TICKETMASTER had been able to locate, along with contact information for the artist and artist management company associated with each ticketing web page, so that TICKETMASTER could identify the Victim Company’s clients and attempt to dissuade them from selling tickets through the Victim Company. A version of the list, which was emailed on or about February 25, 2015, to Coconspirator-1, Zaidi and another TICKETMASTER executive (“Executive-7”), among others, documented 124 URLs for Victim Company ticketing web pages.

46. Coconspirator-1, Zaidi and other TICKETMASTER employees were conscious of the need to prevent the Victim Company from learning that TICKETMASTER was monitoring the Victim Company’s ticketing web pages. For example, on or about August 15, 2014, after Coconspirator-1 sent an email with two URLs for Victim Company ticketing web pages, Zaidi and Executive-6 discussed whether to approach an artist’s manager to inquire about

whether the artist was working with the Victim Company. Zaidi expressed reservations about doing so, explaining that “[t]he problem is we’re not supposed to tip anyone off that we have this view into [the Victim Company’s] activities. We’ll have to keep monitoring.”

47. Similarly, on or about June 3, 2015, after Coconspirator-1 sent an email with two URLs for Victim Company ticketing web pages, another TICKETMASTER employee asked whether he should contact the Victim Company directly. Coconspirator-1 responded, “As they are just test URL’s for now, let’s hold off showing our hand on what we know they’re working on.”

48. Coconspirator-1 and other Live Nation and TICKETMASTER employees also continued to access Victim Company Toolboxes without authorization. Victim Company server log data shows at least 25 discrete instances of access to Victim Company toolboxes between August 2013 and December 2015 from computers accessing the Internet from IP addresses registered to TICKETMASTER and to other Live Nation subsidiaries in New York, San Francisco and Los Angeles. Because the Toolboxes contained information about tours, access to the Toolboxes permitted TICKETMASTER to monitor artists and managers with whom the Victim Company was working.

49. For example, on or about January 16, 2015, Coconspirator-1 forwarded to Executive-7 his January 9, 2014 email to Executive-1 and Zaidi that contained usernames and passwords for three Victim Company Toolboxes. Coconspirator-1 thereafter called Executive-7, who was based in Los Angeles, and offered to show Executive-7 what was “under the hood” of the Victim Company’s Toolboxes. Coconspirator-1 and Executive-7 thereafter both logged into a Toolbox together, and Coconspirator-1 gave Executive-7 a tour of the application. Log data from

the Victim Company reflects that on or about January 16, 2015, an individual using an IP address registered to TICKETMASTER's Los Angeles office and an individual using an IP address registered to a different Live Nation subsidiary simultaneously logged into the same Toolbox.

50. In or about February 2015, Coconspirator-1 gave a group of employees working for Executive-7 a similar demonstration of a Toolbox when Coconspirator-1 visited TICKETMASTER's Los Angeles office. This unauthorized access was similarly documented in the Victim Company's server logs.

IV. The Victim Company Sues Live Nation and TICKETMASTER

51. In or about September 2014, Executive-1 resigned from Live Nation and TICKETMASTER. Executive-1 subsequently began to work for the Victim Company on or about June 16, 2015. After joining the Victim Company, Executive-1 warned the Victim Company to change the sequential numbering system for the Victim Company's ticketing web pages. The Victim Company thereafter changed the way that it generated URLs for its ticketing web pages specifically to prevent Live Nation and TICKETMASTER employees from finding and accessing them.

52. By August 2015, Coconspirator-1 and other TICKETMASTER executives began to notice that they had lost the ability to access Victim Company data and information that they had previously been able to access. In internal emails, Coconspirator-1 and other TICKETMASTER executives attributed their loss of access to Executive-1 warning the Victim Company of their conduct. Specifically, they discussed how the Victim Company had "a really slick web-based demo for clients" which was now "password protected," that TICKETMASTER

“can probably thank [Executive-1] for that one,” and joked that they should email Executive-1 for these new passwords, but that doing so “might raise a red flag.”

53. In or about December 2015, the Victim Company filed a civil complaint against Live Nation and TICKETMASTER alleging antitrust violations, and amended the lawsuit in February 2017 to add allegations that Live Nation and TICKETMASTER had accessed the Victim Company’s computer systems without authorization.

54. In or about January 2018, Live Nation, TICKETMASTER and the Victim Company announced that they had settled the lawsuit, and that Live Nation acquired the Victim Company’s remaining technology assets, including its ticketing commerce platform, patent portfolio and other assets.

ATTACHMENT B

CERTIFICATE OF CORPORATE RESOLUTIONS

WHEREAS, Ticketmaster L.L.C. (the “Company”) has been engaged in discussions with the United States Attorney’s Office for the Eastern District of New York (the “Office”) regarding issues arising in relation to criminal conduct by Company employees for the benefit of the Company; and

WHEREAS, in order to resolve such discussions, it is proposed that the Company enter into a certain agreement with the Office; and

WHEREAS, the Company’s General Counsel, Michael Rowles, together with outside counsel for the Company, has advised the Board of Directors of the Company’s rights, possible defenses, the Sentencing Guidelines’ provisions, and the consequences of entering into such agreement with the Office;

Therefore, the Board of Directors has RESOLVED that:

1. The Company (a) acknowledges the filing of the Information charging the Company with (i) one count of conspiracy to commit offenses against the United States, in violation of Title 18, United States Code, Section 371, that is, to violate provisions of the Computer Fraud and Abuse Act (“CFAA”) as amended, see Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(a)(4); (ii) one substantive count of computer intrusion for commercial advantage or private financial gain, in violation of Title 18, United States Code, Section 1030(a)(2)(C); (iii) one substantive count of computer intrusion in furtherance of fraud, in violation of Title 18, United States Code, Section 1030(a)(4); (iv) one count of conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349; and (v) one

substantive count of wire fraud, in violation of Title 18, United States Code, Section 1343; (b) waives indictment on such charges and enters into a deferred prosecution agreement with the Office; and (c) agrees to accept a monetary penalty against Company totaling \$10,000,000, and to pay such penalty pursuant to Paragraph 10 of the Deferred Prosecution Agreement (“DPA”) to resolve this matter;

2. The Company accepts the terms and conditions of this Agreement, including, but not limited to, (a) a knowing waiver of its rights to a speedy trial pursuant to the Sixth Amendment to the United States Constitution, Title 18, United States Code, Section 3161, and Federal Rule of Criminal Procedure 48(b), and to the statute of limitations under Title 18, United States Code, Section 3282; (b) a knowing waiver, for purposes of this Agreement and any charges by the Office arising out of the conduct described in the Statement of Facts, of any objection with respect to venue; (c) the filing of the Information, as provided under the terms of this Agreement, in the United States District Court for the Eastern District of New York; and (d) a knowing waiver of any defenses based on the statute of limitations for any prosecution relating to the conduct described in the Statement of Facts, or relating to conduct known to the Office prior to the date on which this Agreement was signed, that is not time-barred by the applicable statute of limitations on the date of the signing of this Agreement;

3. The Company’s General Counsel, Michael Rowles, is hereby individually authorized, empowered and directed, on behalf of the Company, to execute the Deferred Prosecution Agreement substantially in such form as reviewed by this Board of Directors at this meeting with such changes as the Company’s General Counsel, Michael Rowles, may approve;

4. The Company's General Counsel, Michael Rowles, is hereby individually authorized, empowered and directed to take any and all actions as may be necessary or appropriate and to approve the forms, terms or provisions of any agreement or other documents as may be necessary or appropriate, to carry out and effectuate the purpose and intent of the foregoing resolutions ; and

5. All of the actions of the Company's General Counsel, Michael Rowles, which actions would have been authorized by the foregoing resolutions except that such actions were taken prior to the adoption of such resolutions, are hereby severally ratified, confirmed, approved, and adopted as actions on behalf of the Company.

Date: 12/29/2020

By: _____
Michael Rowles
General Counsel
Ticketmaster L.L.C.

ATTACHMENT C

CORPORATE COMPLIANCE PROGRAM

In order to address any deficiencies in its internal controls, compliance code, policies, and procedures regarding compliance with the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, and other applicable computer crime laws, Ticketmaster L.L.C. (the “Company”) agrees to continue to conduct, in a manner consistent with all of its obligations under this Agreement, appropriate reviews of its existing internal controls, policies and procedures.

Where necessary and appropriate, the Company agrees to modify or maintain its existing compliance program, including internal controls, compliance policies and procedures, in order to ensure that the program is effectively designed to prevent, detect and deter violations of the CFAA and other applicable computer crime laws, or the unauthorized and unlawful acquisition of confidential information belonging to the Company’s competitors. At a minimum, the Company’s compliance program must include the following elements:

Commitment to Compliance

1. The Company will ensure that its directors and senior management provide clear and explicit support and commitment to its corporate policies and compliance codes against violations of the computer crime laws and against the unauthorized and unlawful acquisition of confidential information belonging to its competitors, and that they will demonstrate adherence by example. The Company will also provide managerial training designed to ensure that middle management, in turn, reinforces those standards and encourages employees to abide by them. The Company will create and foster a culture of ethics and compliance with the law in its day-to-day operations at all levels of the company.

Policies and Procedures

2. The Company will maintain clearly articulated and visible corporate policies against violations of the CFAA and other applicable computer crime-related laws (collectively, the “computer crime laws”) and against the unauthorized and unlawful acquisition of confidential information belonging to the Company’s competitors (“competitor confidential information”), which policies shall be memorialized in a written compliance code or codes.

3. These policies and procedures shall apply to all directors, officers and employees and, where necessary and appropriate, outside parties acting on behalf of the Company, including, but not limited to, agents and intermediaries, consultants, representatives, distributors, teaming partners, contractors and suppliers, consortia and joint venture partners (collectively, “agents and business partners”). The Company shall notify all employees that compliance with the policies and procedures is the duty of individuals at all levels of the company. Such policies and procedures shall address, at a minimum:

- a. Intentional access to a computer without authorization or intentional access that exceeds authorized access to a computer;
- b. Intentional access to a computer for the purpose of deceiving or defrauding someone;
- c. Misuse or trafficking of passwords or similar information through which a computer may be accessed without authorization;
- d. The need for former employees, contractors or agents of competitors who are hired or contracted to work for the Company to continue to protect the confidentiality of competitor confidential information obtained during their previous employment or contractual relationship;
- e. The need for managers and executives of the Company to ensure that former employees, contractors or agents of competitors who are hired or contracted to work for the Company are not asked to unlawfully provide or make use

of, and do not volunteer to unlawfully disclose, competitor confidential information;

4. The Company has represented that it has put technical controls in place to block employees from using the Company's corporate systems to access password-protected areas of competitor websites, except where employees have a valid business need and authorization to do so. The Company will ensure that it will maintain these controls as a means of preventing violations of the CFAA and other computer crime laws and protecting the confidentiality of competitor confidential information. The Company will maintain these technical controls, review their efficacy as part of part of the periodic risk-based review required below, and when necessary implement additional mechanisms designed to effectively enforce its compliance code, policies, and procedures, including appropriately incentivizing compliance and disciplining violations.

Periodic Risk-Based Review

5. The Company will conduct a periodic risk assessment of these compliance policies and procedures addressing the individual circumstances of the Company.

6. The Company shall review its computer crime and competitor confidential information compliance policies and procedures no less than annually and update them as appropriate to ensure their continued effectiveness, taking into account relevant developments in the field and evolving international and industry standards.

Proper Oversight and Independence

7. The Company will assign responsibility to one or more senior corporate executives of the Company for the implementation and oversight of the Company's computer crime and competitor confidential information compliance code, policies and procedures. Such corporate official(s) shall have the authority to report directly to independent monitoring bodies, including

internal audit, the Company's Board of Directors, or any appropriate committee of the Board of Directors, and shall have an adequate level of stature and autonomy from management as well as sufficient resources and authority to maintain such autonomy.

Training and Guidance

8. The Company will implement training and guidance designed to ensure that its computer crime and competitor confidential information compliance code, policies and procedures are effectively communicated to all directors, officers, employees, and, where necessary and appropriate, agents and business partners. These mechanisms shall include: (a) periodic training for all directors and officers, all employees in positions of leadership or trust, positions that require such training (e.g., internal audit, sales, legal, compliance, finance), or positions that otherwise pose such risk to the Company, and, where necessary and appropriate, agents and business partners; and (b) corresponding certifications by all such directors, officers, employees, agents, and business partners, certifying compliance with the training requirements. The Company will conduct training in a manner tailored to the audience's size, sophistication, or subject matter expertise and, where appropriate, will discuss prior compliance incidents.

9. The Company will maintain, or where necessary establish, an effective system for providing guidance and advice to directors, officers, employees, and, where necessary and appropriate, agents and business partners, about complying with the Company's computer crime and competitor confidential information compliance code, policies, and procedures, including when they need advice on an urgent basis.

Internal Reporting and Investigation

10. The Company will maintain, or where necessary establish, an effective system for internal and, where possible, confidential reporting by, and protection of, directors, officers, employees, and, where appropriate, agents and business partners, concerning violations of the computer crime laws or the Company's computer crime and competitor confidential information compliance code, policies, and procedures.

11. The Company will maintain, or where necessary establish, an effective and reliable process with sufficient resources for responding to, investigating, and documenting allegations of violations of the computer crime laws or the Company's computer crime and competitor confidential information compliance code, policies, and procedures. The Company will handle the investigations of such complaints in an effective manner, including routing the complaints to proper personnel, conducting timely and thorough investigations, and following up with appropriate discipline where necessary.

Enforcement and Discipline

12. The Company will maintain appropriate disciplinary procedures to address, among other things, violations of the computer crime laws, the unauthorized and unlawful acquisition of competitor confidential information and violations of the Company's computer crime and competitor confidential information compliance code, policies, and procedures by the Company's directors, officers and employees. Such procedures should be applied consistently, fairly and in a manner commensurate with the violation, regardless of the position held by, or perceived importance of, the director, officer or employee. The Company shall implement procedures to ensure that where misconduct is discovered, reasonable steps are taken to remedy

the harm resulting from such misconduct, and to ensure that appropriate steps are taken to prevent further similar misconduct, including assessing the internal controls, compliance code, policies and procedures, and making modifications necessary to ensure the overall computer crime and competitor confidential information compliance program is effective.

Third-Party Relationships

13. The Company will institute appropriate risk-based due diligence and compliance requirements pertaining to the retention and oversight of all agents and business partners, including, where necessary and appropriate:

a. properly documented due diligence pertaining to the hiring and appropriate and regular oversight of agents and business partners;

b. informing agents and business partners of the Company's commitment to abiding by computer crime laws, protecting competitor confidential information and of the Company's computer crime and competitor confidential information compliance code, policies, and procedures;

c. seeking a reciprocal commitment from agents and business partners; and

d. including standard provisions in agreements, contracts and renewals thereof with all agents and business partners that are reasonably calculated to prevent violations of the computer crime laws and to prevent the unauthorized and unlawful acquisition of competitor confidential information, which may, depending upon the circumstances, include: (i) representations and undertakings relating to compliance with the computer crime laws and the protection of competitor confidential information; and (ii) rights to terminate an agent or business partner as a result of any breach of the computer crime laws or the unauthorized and unlawful

acquisition of competitor confidential information, the Company's compliance code, policies or procedures, or the representations and undertakings related to such matters.

Mergers and Acquisitions

14. The Company will develop and implement policies and procedures for mergers and acquisitions requiring that the Company conduct appropriate risk-based due diligence on potential new business entities, including appropriate computer crime and competitor confidential information due diligence by legal and compliance personnel.

15. The Company will ensure that the Company's compliance code, policies and procedures regarding the computer crime laws and competitor confidential information apply as quickly as is practicable to newly acquired businesses or entities merged with the Company and will promptly:

a. train the directors, officers, employees, agents and business partners consistent with Paragraph 8 above on the computer crime laws and the Company's compliance code, policies, and procedures regarding computer crime laws and competitor confidential information; and

b. where warranted, conduct a CFAA-specific audit of all newly acquired or merged businesses as quickly as practicable.

Monitoring, Testing and Remediation

16. In order to ensure that its compliance program does not become stale, the Company will conduct periodic reviews and testing of its computer crime and competitor confidential information compliance codes, policies and procedures designed to evaluate and improve their effectiveness in preventing and detecting violations of computer crime laws, the

unauthorized and unlawful acquisition of competitor confidential information and the Company's computer crime and competitor confidential information codes, policies and procedures, taking into account relevant developments in the field and evolving international and industry standards. The Company will ensure that compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing. Based on such review and testing and its analysis of any prior misconduct, the Company will conduct a thoughtful root cause analysis and timely and appropriately remediate to address the root causes.

ATTACHMENT D

REPORTING REQUIREMENTS

The Company agrees that it will report to the Office periodically, at no less than twelve-month intervals during a three-year term, regarding remediation and implementation of the compliance program and internal controls, policies, and procedures described in Attachment C. During this three-year period, the Company shall: (1) conduct an initial review and submit an initial report, and (2) conduct and prepare at least two follow-up reviews and reports, as described below:

a. By no later than one year from the date this Agreement is executed, the Company shall submit to the Office a written report setting forth a complete description of its remediation efforts to date, its proposals, if any, reasonably designed to improve the Company's internal controls, policies and procedures for ensuring compliance with the CFAA, other applicable computer crime-related laws, and the protection of competitor confidential information, and the proposed scope of the subsequent reviews. The report shall be transmitted to Chief, National Security and Cybercrime Section, U.S. Attorney's Office for the Eastern District of New York, 271-A Cadman Plaza East, Brooklyn, New York, 11201. The Company may extend the time period for issuance of the report with prior written approval of the Office.

b. The Company shall undertake at least two follow-up reviews and reports, incorporating the Office's views on the Company's prior reviews and reports, to further monitor and assess whether the Company's policies and procedures are reasonably designed to detect and prevent violations of the CFAA and other applicable computer crime laws and to prevent the unauthorized and unlawful acquisition of competitor confidential information.

c. The first follow-up review and report shall be completed by no later than one year after the initial report is submitted to the Office. The second follow-up review and report shall be completed and delivered to the Office no later than thirty days before the end of the Term.

d. The reports will likely include proprietary, financial, confidential and/or competitive business information. Moreover, public disclosure of the reports could discourage cooperation, impede pending or potential government investigations and thus undermine the objectives of the reporting requirement. For these reasons, among others, the reports and the contents thereof are intended to remain and shall remain non-public, except as otherwise agreed to by the parties in writing, or except to the extent that the Office determines in its sole discretion that disclosure would be in furtherance of the Office's discharge of its duties and responsibilities or is otherwise required by law.

e. The Company may extend the time period for submission of any of the follow-up reports with prior written approval of the Office.

ATTACHMENT E

CERTIFICATION

To: United States Attorney's Office
Eastern District of New York
Attention: Chief – National Security and Cybercrime Section

Re: Deferred Prosecution Agreement Disclosure Certification

The undersigned certify, pursuant to Paragraph 22 of the Deferred Prosecution Agreement (“DPA”) filed on December 30, 2020, in the U.S. District Court for the Eastern District of New York, by and between the United States and Ticketmaster L.L.C. (the “Company”), that the undersigned are aware of the Company’s disclosure obligations under Paragraph 6 of the DPA and that undersigned have disclosed to the United States Attorney’s Office for the Eastern District of New York (the “Office”) any and all evidence or allegations of conduct required pursuant to Paragraph 6 of the DPA, which includes evidence or allegations that may constitute a violations of the CFAA or the wire fraud statute (“Disclosable Information”). This obligation to disclose information extends to any and all Disclosable Information that has been identified through the Company’s compliance and controls program, whistleblower channel, internal audit reports, due diligence procedures, investigation process, or other processes. The undersigned further acknowledge and agree that the reporting requirement contained in Paragraph 6 and the representations contained in this certification constitute a significant and important component of the DPA and the Office’s determination whether the Company has satisfied its obligations under the DPA.

The undersigned hereby certify, respectively, that he is the President of the Company and that he is the Chief Compliance Officer (“CCO”) of the Company and that each has been duly authorized by the Company to sign this Certification on behalf of the Company.

This Certification shall constitute a material statement and representation by the undersigned and by, on behalf of, and for the benefit of, the Company to the executive branch of the United States for purposes of 18 U.S.C. § 1001, and such material statement and representation shall be deemed to have been made in the Eastern District of New York. This Certification shall also constitute a record, document, or tangible object in connection with a matter within the jurisdiction of a department and agency of the United States for purposes of 18 U.S.C. § 1519, and such record, document, or tangible object shall be deemed to have been made in the Eastern District of New York.

Date: _____

By: _____

President

Date: _____

By: _____

Chief Compliance Officer