COTCHETT, PITRE & McCARTHY, LLP
Thomas E. Loeser (*SBN: 202724*)
Karin B. Swope (*pro hac vice to be filed)*
999 N. Northlake Way, Suite 215
Seattle, WA 98103
Tel: (206) 802-1272
Fax: (650) 697-0577
Email: tloeser@cpmlegal.com
kswope@cpmlegal.com

Attorneys for Plaintiffs James Curry and David Freifeld the proposed Class

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

JAMES CURRY and DAVID FREIFELD, on behalf of themselves and a class of similarly situated persons,

Plaintiffs,

v.

TICKETMASTER, LLC and LIVE NATION ENTERTAINMENT, INC.,

Defendants.

NO.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

Plaintiffs James Curry and David Freifeld, individually and on behalf of all others similarly situated ("Plaintiffs"), bring this action against Defendant Ticketmaster LLC ("Ticketmaster") and Defendant Live Nation Entertainment, Inc. ("Live Nation") (collectively, "Defendants"), seeking monetary damages, restitution, and/or injunctive relief for the proposed Class and Subclasses, as defined below. Plaintiffs make the following allegations upon information and belief, the investigation of their counsel, and personal knowledge or facts that are a matter of public record.

I. INTRODUCTION

1. The release, disclosure, and publication of sensitive, private data can be devasting. Not only is it an intrusion of privacy and a loss of control, but it is a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.[1] A data breach can have a grave consequences for victims for years after the actual date of the breach—with the obtained information, thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, obtain government benefits, and/or obtain driver's licenses in the victims' names, forcing victims to maintain a constant vigilance over the potential misuse of their information.

2. Beverly Hills, California based Ticketmaster is a wholly owned subsidiary of Live Nation and markets itself as a sophisticated, reliable entertainment ticket seller. Live Nation is "the largest live entertainment company in the world, connecting over 765 million fans across all of our concerts and ticketing platforms in 49 countries during 2023."[2] In its Privacy Policy found on its website, Live Nation has a section entitled "Looking After Your Information," under which it claims" "We take steps to try to make sure your information is protected and to delete it securely when we no longer need it."[3]

---

[1] Dave Maxfield & Bill Latham, Data Breaches: Perspectives from Both Sides of the Wall, S.C. Lawyer (May 2014).

[2] Form 10-K Annual Report for Live Nation Entertainment, Inc., BAMSEC, https://www.bamsec.com/filing/133525824000017?cik=1335258 (last visited June 4, 2024).

[3] *Live Nation Privacy Policy*, LIVE NATION, available online at https://help.livenation.com/hc/en-us/articles/10464047306641-Live-Nation-Entertainment-Privacy-Policy#security (last visited June 4, 2024).

3. Despite these representations, Defendants' protection of the information it maintains from and about its customers was woefully inadequate. On May 27, 2024, renowned hacking group ShinyHunters offered 1.3 terabytes of Class members' personal and financial information for sale for $500,000.[4] According to ShinyHunters, they had possession of individuals' personal identifiable information ("PII"), including but not limited to "full names, addresses, email addresses, phone numbers, ticket sales and event details, order information, and partial payment card data. [The] compromised payment data includes customer names, the last four digits of card numbers, expiration dates, and even customer fraud details."[5]

4. On May 29, 2024, Live Nation confirmed in a brief Form 8-k filing with the SEC that on May 20, 2024, it discovered that a third-party database containing its customers' private information had been breached.[6] Specifically, the disclosure form stated:

> On May 20, 2024, Live Nation Entertainment, Inc. (the "Company" or "we") identified unauthorized activity within a third-party cloud database environment containing Company data (primarily from its Ticketmaster L.L.C. subsidiary) and launched an investigation with industry-leading forensic investigators to understand what happened. On May 27, 2024, a criminal threat actor offered what it alleged to be Company user data for sale via the dark web. We are working to mitigate risk to our users and the Company, and have notified and are cooperating with law enforcement. As appropriate, we are also notifying regulatory authorities and users with respect to unauthorized access to personal information.[7]

5. Defendants apparently had no idea that a system containing Class members' PII had been infiltrated and the personal and private information of some 560 million persons had been exfiltrated, until the information was offered for sale on the Dark Web. This fact alone portends Defendants' protection systems and protocols were inadequate.

---

[4] Waqas, *Hackers Claim Ticketmaster Data Breach: 560M Users' Info for Sale at $500k*, HACKREAD (May 29, 2024), available online at https://hackread.com/hackers-ticketmaster-data-breach- 560m-users-sale/

[5] *Id.*

[6] *See Form 8-k, available online at: https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm* .

[7] *Id.*

6. As a result of the Data Breach, through which their Personally Identifiable Information ("PII") was compromised, disclosed, and obtained by unauthorized third parties, Plaintiffs and Class Members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud and identity theft for a period of years, if not decades. Furthermore, Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft, at their own expense. Consequently, Plaintiffs and the other Class Members will incur ongoing out-of-pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

7. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

II. JURISDICTION, VENUE, AND CHOICE OF LAW

8. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711, *et seq.*, because at least one member of the Class, as defined below, is a citizen of a different state than Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs. This Court also has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a).

9. This Court has jurisdiction over Defendant Ticketmaster because Ticketmaster has committed acts with this District giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Ticketmaster would not offend traditional notions of fair play and substantial justice. Ticketmaster has its headquarters in this District and has engaged in continuous, systematic, and substantial activities within the State of California, including substantial marketing and sales of services and products in connection with the Data Breach within California.

10. The Court has jurisdiction over Defendant Live Nation, Inc. because Live Nation maintains its principal place of business in this District, has sufficient minimum contacts with

this District, and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

11. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Live Nation's and Ticketmaster's principal place of business is located in this District and a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

III. PARTIES

A. Plaintiff James Curry

12. Plaintiff James Curry is a citizen of and is domiciled in Los Angeles in the state of California.

13. Plaintiff is a customer of Ticketmaster and has purchased tickets from Ticketmaster.

14. Plaintiff provided confidential and sensitive PII to Ticketmaster, as requested and required by Ticketmaster for the provision of its services. Ticketmaster obtained and continues to maintain Plaintiff's PII and has a legal duty and obligation to protect that PII from unauthorized access and disclosure.

15. Plaintiff would not have entrusted his PII to Ticketmaster had he known that Ticketmaster failed to maintain adequate data security.

16. On or about June 2, 2024, plaintiff read an article online that indicated that Ticketmaster had lost the information of 560 million customers, and thus his information was compromised.

17. Plaintiff subsequently spent several hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect himself from data breaches, and reviewing his financial accounts for fraud or suspicious activity. He now plans to spend several hours a month checking account statements for irregularities.

18. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of his PII, which he expected Defendants to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his PII. As

a result of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

B. Plaintiff David Freifeld

19. Plaintiff David Freifeld is a citizen of and is domiciled in Vernon Hills in the state of Illinois.

20. Plaintiff is a customer of Ticketmaster and has purchased on average 3-4 sets of tickets per year from Ticketmaster over at least the last several years.

21. Plaintiff provided confidential and sensitive PII to Ticketmaster, as requested and required by Ticketmaster for the provision of its services. Ticketmaster obtained and continues to maintain Plaintiff's PII and has a legal duty and obligation to protect that PII from unauthorized access and disclosure.

22. Plaintiff would not have entrusted his PII to Ticketmaster had he known that Ticketmaster failed to maintain adequate data security.

23. On or about June 4, 2024, plaintiff read an article online that indicated that Ticketmaster had lost the information of 560 million customers, and thus his information was compromised.

24. Plaintiff subsequently spent several hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect himself from data breaches, and reviewing his financial accounts for fraud or suspicious activity. He now plans to spend several hours a month checking account statements for irregularities.

25. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of his PII, which he expected Defendants to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his PII. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

C. Defendants

26. Defendant Ticketmaster, LLC is a wholly owned subsidiary of Defendant Live Nation Entertainment, Inc. headquartered in California with its principal executive office at 9348 Civic Center Drive, Beverly Hills, California.

27. In the course of its business, Ticketmaster collects names, phone numbers, Social Security numbers, physical addresses, driver's license information, and other information from its customers and prospective customers.

28. Defendant Live Nation Entertainment, Inc. is a Delaware corporation headquartered in California with its principal executive office at 9348 Civic Center Drive, Beverly Hills, California.

29. In the course of its business, Live Nation collects names, phone numbers, Social Security numbers, physical addresses, driver's license information, and other information from its customers and prospective customers.

IV. FACTUAL BACKGROUND

A. Defendants Failed to Adequately Protect Customer Data, Resulting in the Data Breach

30. On May 28, 2024, ShinyHunters, a known criminal hacking group, posted for sale 1.3 terabytes of PII on a hacker forum and marketplace.[8] According to ShinyHunters' forum post, the PII included "560 million customers [*sic*] full details (name, address, email, phone) [¶] Ticket sales, event information, order details [¶] CC [credit card] detail [*sic*] [¶] customer, last 4 of card, expiration date. Customer fraud details [¶] much more."[9] ShinyHunters offered to sell the data for $500,000.[10]

31. On May 29, 2024, Live Nation made a Form 8-k filing with the SEC reporting that on May 20, 2024, it discovered that its customers' private information had been offered for

[8] Waqas, *Hackers Claim Ticketmaster Data Breach: 560M Users' Info for Sale at $500k*, HACKREAD (June 3, 2024), https://hackread.com/hackers-ticketmaster-data-breach- 560m-users-sale/.

[9] *Id.*

[10] *Id.*

sale. The disclosure stated that Live Nation had "identified unauthorized activity within a third-party cloud database environment containing Company data (primarily from its Ticketmaster L.L.C. subsidiary) and launched an investigation with industry-leading forensic investigators to understand what happened."[11] The disclosure further stated that Live Nation was "working to mitigate risk to our users and the Company[.]"[12]

32. Defendants were familiar with their obligations—created by contract, industry standards, common law, and representations to their customers—to protect customer information. Plaintiffs and Class Members provided their PII to Defendants with the reasonable expectation that Defendants would comply with its obligations to keep such information confidential and secure.

33. Ticketmaster states on its website: "We're always taking steps to make sure your information is protected and deleted securely" and "[w]e have security measures in place to protect your information."[13]

34. Ticketmaster also sets forth "10 commitments" on its website, including its purported commitment to "Security & Confidentiality."[14] Specifically, Ticketmaster asserts that "[t]he security of our fans' information is a priority for us. We take all necessary security measures to protect personal information that's shared and stored with us."[15]

35. Defendants failed to comply with these obligations, resulting in the Data Breach. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records.

B. The Data Breach Puts Consumers at Increased Risk of Fraud and Identity Theft

36. An identity thief uses victims' PII, such as name, address, and other sensitive and confidential information, without permission, to commit fraud or other crimes that range from

[11] *See* Form 8-k, attached as Exhibit A.

[12] *Id.*

[13] *Privacy Policy*, TICKETMASTER, https://privacy.ticketmaster.com/privacy-policy (last visited June 4, 2024).

[14] *Our Commitments*, TICKETMASTER, https://privacy.ticketmaster.com/en/our-commitments (last visited June 4, 2024).

[15] *Id.*

immigration fraud, obtaining a driver's license or identification card, obtaining government benefits, and filing fraudulent tax returns to obtain tax refunds.

37. Identity thieves can use a victim's PII to open new financial accounts, incur charges in the victim's name, take out loans in the victim's name, and incur charges on existing accounts of the victim. Plaintiffs' finances are now at risk due to the Data Breach.

38. Identity theft is the most common consequence of a data breach—it occurs to 65% of data breach victims.[16] Consumers lost more than $56 billion to identity theft and fraud in 2020, and over 75% of identity theft victims reported emotional distress.[17]

39. Plaintiffs are now in the position of having to take steps to mitigate the damages caused by the Data Breach. Once use of compromised non-financial PII is detected, the emotional and economic consequences to the victims are significant. Studies done by the ID Theft Resource Center, a non-profit organization, found that victims of identity theft had marked increased fear for personal financial security. The report attributes this to more people having been victims before, contributing to greater awareness and understanding that they may suffer long term consequences from this type of crime.[18]

40. Ticketmaster failed to protect and safeguard Plaintiffs' and Class Members' private information, in fact failing to adhere to even its most basic obligations. As a result, Plaintiffs and Class Members have suffered or will suffer actual injury, including loss of privacy, costs, and loss of time.

V. CLASS ACTION ALLEGATIONS

41. Plaintiffs brings this action as a class action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of a proposed nationwide class (the "Class"), defined as:

> All natural persons in the United States whose Personally Identifiable Information was compromised as a result of the Data Breach.

---

[16] Eugene Bekker, *What Are Your Odds of Getting Your Identity Stolen?*, IDENTITYFORCE (Apr. 15, 2021), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics (last visited Feb. 1, 2023).

[17] *Id.*

[18] Identity Theft: The Aftermath 2013, Identity Theft Resource Center, https://idtheftinfo.org/latest-news/72 (last visited Feb. 1, 2023).

42. In addition, the State Subclasses are defined as follows:

> **California Subclass:** All natural persons in the State of California whose Personally Identifiable Information was compromised as a result of the Data Breach.
>
> **Illinois Subclass:** All natural persons in the State of Illinois whose Personally Identifiable Information was compromised as a result of the Data Breach.

43. **Numerosity and Ascertainability:** Plaintiffs do not know the exact size of the Class or identity of the Class Members, since such information is in the exclusive control of Defendants. Nevertheless, the Class, on information and belief includes millions of individuals dispersed throughout the United States, considering approximately 560 million Ticketmaster customers' information was reportedly subject to unauthorized access. The number of Class Members is so numerous that joinder of all Class Members is impracticable. The names, addresses, and phone numbers of Class Members are identifiable through documents maintained by Defendants.

44. **Commonality and Predominance:** This action involves common questions of law and fact which predominate over any question solely affecting individual Class Members. These common questions include:

A. whether Defendants engaged in the conduct alleged herein;

B. whether Defendants had a legal duty to use reasonable security measures to protect Plaintiffs' and Class Members' PII;

C. whether Defendants timely, accurately, and adequately informed Plaintiffs and Class Members that their PII had been compromised;

D. whether Defendants breached their legal duty by failing to protect the PII of Plaintiffs and Class Members;

E. whether Defendants acted reasonably in securing the PII of Plaintiffs and Class Members;

F. whether Plaintiffs and Class Members are entitled to injunctive relief;

G. and whether Plaintiffs and Class Members are entitled to damages and equitable relief.

45. **Typicality:** Plaintiffs' claims are typical of the other Class Members' claims because all Class Members were comparably injured through Defendants' substantially uniform misconduct, as described above. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other members of the Class that they represent, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and Class Members arise from the same operative facts and are based on the same legal theories.

46. **Adequacy:** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other members of the Class they seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; and Plaintiffs intend to prosecute this action vigorously. The Class's interest will be fairly and adequately protected by Plaintiffs and their counsel.

47. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other detriment suffered by Plaintiffs and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be virtually impossible for the Class Members to individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not: individualized litigation creates a potential for inconsistent or contradictory judgments, increases the delay and expense to the parties, and increases the expense and burden to the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by this Court.

VI. CAUSES OF ACTION

A. Claims Brought on Behalf of the Nationwide Class

COUNT ONE
NEGLIGENCE

48. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

49. Ticketmaster owed a duty to Plaintiffs and Class Members, arising from the sensitivity of the information, the expectation the information was going to be kept private, and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, implementing, maintaining, monitoring, and testing Ticketmaster's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class Members' information was adequately secured from unauthorized access.

50. Ticketmaster's Privacy Notice acknowledged Ticketmaster's duty to adequately protect Plaintiffs' and Class Members' PII.

51. Ticketmaster owed a duty to Plaintiffs and Class Members to implement administrative, physical and technical safeguards, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiffs' and Class Members' PII.

52. Ticketmaster also had a duty to only maintain PII that was needed to serve customer needs.

53. Ticketmaster owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII.

54. Ticketmaster also had independent duties under Plaintiffs' and Class Members' state laws that required Ticketmaster to reasonably safeguard Plaintiffs' and Class Members' PII, and promptly notify them about the Data Breach.

55. Ticketmaster had a special relationship with Plaintiffs and Class Members as a result of being entrusted with their PII, which provided an independent duty of care. Plaintiffs' and Class Members' willingness to entrust Ticketmaster with their PII was predicated on the understanding that Ticketmaster would take adequate security precautions. Moreover, Ticketmaster was capable of protecting its networks and systems, and the PII it stored on them, from unauthorized access.

56. Ticketmaster breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Plaintiffs' and Class Members' PII,

including administrative, physical, and technical safeguards; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII.

57. But for Ticketmaster's breach of its duties, including its duty to use reasonable care to protect and secure Plaintiffs' and Class Members' PII, Plaintiffs' and Class Members' PII would not have been accessed by unauthorized parties.

58. Plaintiffs and Class Members were foreseeable victims of Ticketmaster's inadequate data security practices. Ticketmaster knew or should have known that a breach of its data security systems would cause damage to Plaintiffs and Class Members.

59. It was reasonably foreseeable that the failure to reasonably protect and secure Plaintiffs' and Class Members' PII would result in unauthorized access to Ticketmaster's networks, databases, and computers that stored or contained Plaintiffs' and Class Members' PII.

60. As a result of Ticketmaster's negligent failure to prevent the Data Breach, Plaintiffs and Class Members suffered injury, which includes, but is not limited to, exposure to a heightened and imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members have also incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter and detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of the PII.

61. The harm to Plaintiffs and Class Members was a proximate, reasonably foreseeable result of Ticketmaster's breaches of its aforementioned duties.

62. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT TWO
NEGLIGENCE PER SE

63. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

64. Under the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Ticketmaster had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

65. In addition, under state data security statutes, Ticketmaster had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII.

66. Ticketmaster breached its duties to Plaintiffs and Class Members, under the Federal Trade Commission Act, 15 U.S.C. § 45, ("FTCA") and the state data security statutes, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

67. Plaintiffs and Class Members were foreseeable victims of Ticketmaster's violations of the FTCA and state data security statutes. Ticketmaster knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiffs' and Class Members' PII would cause damage to Plaintiffs and Class Members.

68. Ticketmaster's failure to comply with the applicable laws and regulations constitutes negligence *per se.*

69. But for Ticketmaster's violation of the applicable laws and regulations, Plaintiffs' and Class Members' PII would not have been accessed by unauthorized parties.

70. As a result of Ticketmaster's failure to comply with applicable laws and regulations, Plaintiffs and Class Members suffered injury, which includes but is not limited to the exposure to a heightened and imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of the PII.

71. The harm to Plaintiffs and the Class Members was a proximate, reasonably foreseeable result of Ticketmaster's breaches of the applicable laws and regulations.

72. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT THREE
GROSS NEGLIGENCE

73. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

74. Plaintiffs and Class Members entrusted Ticketmaster with highly sensitive and inherently personal private data subject to confidentiality laws.

75. In requiring, obtaining and storing Plaintiffs' and Class Members' PII, Ticketmaster owed a duty of reasonable care in safeguarding the PII.

76. Ticketmaster's networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiffs' and Class Members' PII were secured from unauthorized access.

77. Ticketmaster's networks, systems, protocols, policies, procedures and practices, as described above, were not reasonable given the sensitivity of the Plaintiffs' and Class Members' private data and the known vulnerabilities of Ticketmaster's systems.

78. Ticketmaster did not comply with state and federal laws and rules concerning the use and safekeeping of this private data.

79. Upon learning of the Data Breach, Ticketmaster should have immediately disclosed the Data Breach to Plaintiffs and Class Members, credit reporting agencies, the Internal Revenue Service, financial institutions and all other third parties with a right to know and the ability to mitigate harm to Plaintiffs and Class Members as a result of the Data Breach.

80. Despite knowing its networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiffs' and Class Members' PII were secured from unauthorized access, Ticketmaster ignored the inadequacies and was oblivious to the risk of unauthorized access it had created.

81. Ticketmaster's behavior establishes facts evidencing a reckless disregard for Plaintiffs' and Class Members' rights.

82. Ticketmaster, therefore, was grossly negligent.

83. Ticketmaster's negligence also constitutes negligence per se.

84. The negligence is directly linked to injuries.

85. As a result of Ticketmaster's reckless disregard for Plaintiffs' and Class Members' rights by failing to secure their PII, despite knowing its networks, systems, protocols, policies, procedures and practices were not adequately designed, implemented, maintained, monitored and tested, Plaintiffs and Class Members suffered injury, which includes but is not limited to the exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiffs and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of the PII.

86. The harm to Plaintiffs and the Class Members was a proximate, reasonably foreseeable result of Ticketmaster's breaches of the applicable laws and regulations.

87. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

COUNT FOUR
BREACH OF EXPRESS CONTRACTS

88. Plaintiffs reallege and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

89. Plaintiffs and members of the Class, additionally and alternatively, allege that they entered into valid and enforceable express contracts with Ticketmaster.

90. Under these express contracts, Ticketmaster promised and was obligated to: (a) provide services to Plaintiffs and Class Members; and (b) protect Plaintiffs' and the Class

Members' PII. In exchange, Plaintiffs and members of the Class agreed to pay money for these services.

91. Both the provision of services, as well as the protection of Plaintiffs' and Class Members' PII, were material aspects of these contracts.

92. Ticketmaster's express representations, including, but not limited to, express representations found in Ticketmaster's Privacy Notice, formed an express contract requiring Ticketmaster to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII.

93. Alternatively, the express contracts included implied terms requiring Ticketmaster to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII, including in accordance with federal, state and local laws, and industry standards.

94. Consumers value their privacy, the privacy of their dependents, and the ability to keep their PII associated with obtaining services private. To customers such as Plaintiffs and Class Members, services that do not adhere to industry-standard data security protocols to protect PII are fundamentally less useful and less valuable than services that adhere to industry-standard data security. Plaintiffs and Class Members would not have entered into these contracts with Ticketmaster without an understanding that their PII would be safeguarded and protected.

95. A meeting of the minds occurred, as Plaintiffs and members of the Class provided their PII to Ticketmaster and paid for the provided services in exchange for, amongst other things, protection of their PII.

96. Ticketmaster materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Specifically, Ticketmaster did not comply with federal, state and local laws, or industry standards, or otherwise protect Plaintiffs' and the Class Members' PII, as set forth above. Further, on information and belief, Ticketmaster has not yet provided Data Breach notifications to some affected Class Members who may already be victims of identity fraud or theft or are at imminent risk of becoming

victims of identity theft or fraud associated with PII that they provided to Ticketmaster. These Class Members are as yet unaware of the potential source for the compromise of their PII.

97. The Data Breach was a reasonably foreseeable consequence of Ticketmaster's actions in breach of these contracts.

98. As a result of Ticketmaster's failure to fulfill the data security protections promised in these contracts, Plaintiffs and members of the Class did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in the contracts. Plaintiffs and Class Members, therefore, were damaged in an amount at least equal to the difference in the value of the secure services they paid for and the services they received.

99. Had Ticketmaster disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither Plaintiffs, nor Class Members, nor any reasonable person would have purchased services from Ticketmaster.

100. As a result of Ticketmaster's breach, Plaintiffs and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain in imminent risk of suffering additional damages in the future.

101. As a result of Ticketmaster's breach, Plaintiffs and the Class Members have suffered actual damages resulting from their attempt to mitigate the effects of the breach of contract and subsequent Data Breach, including but not limited to, taking steps to protect themselves from the loss of their PII.

102. Accordingly, Plaintiffs and the other members of the Class have been injured as a result of Ticketmaster's breach of contracts and are entitled to damages and/or restitution in an amount to be determined at trial.

COUNT FIVE
BREACH OF IMPLIED CONTRACTS

103. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

104. Plaintiffs and Class Members were required to provide their PII to obtain services from Ticketmaster. Plaintiffs and Class Members entrusted their PII to Ticketmaster in order to obtain services from them.

105. By providing their PII, and upon Ticketmaster's acceptance of such information, Plaintiffs and Class Members on one hand, and Ticketmaster on the other hand, entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the services provided, whereby Ticketmaster was obligated to take reasonable steps to secure and safeguard that information.

106. Ticketmaster had an implied duty of good faith to ensure that the PII of Plaintiffs and Class Members in its possession was only used in accordance with their contractual obligations.

107. Ticketmaster was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' PII and to comply with industry standards and state laws and regulations for the security of this information, and Ticketmaster expressly assented to these terms in its Privacy Notice as alleged above.

108. Under these implied contracts for data security, Ticketmaster was further obligated to provide Plaintiffs and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

109. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Ticketmaster, including paying for the services provided by Ticketmaster and/or providing the PII required by Ticketmaster.

110. Ticketmaster breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' PII, resulting in the Data Breach. Ticketmaster unreasonably interfered with the contract benefits owed to Plaintiffs and Class Members.

111. Further, on information and belief, Ticketmaster has not yet provided Data Breach notifications to affected Class Members who may already be victims of identity fraud or theft, or are at imminent risk of becoming victims of identity theft or fraud, associated with the PII that they provided to Ticketmaster. These Class Members are unaware of the potential source for the compromise of their PII.

112. The Data Breach was a reasonably foreseeable consequence of Ticketmaster's actions in breach of these contracts.

113. As a result of Ticketmaster's conduct, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received services that were of a diminished value as compared to the secure services they paid for. Plaintiffs and Class Members, therefore, were damaged in an amount at least equal to the difference in the value of the secure services they paid for and the services they received.

114. Neither Plaintiffs, nor Class Members, nor any reasonable person would have provided their PII to Ticketmaster had Ticketmaster disclosed that its security was inadequate or that it did not adhere to industry-standard security measures.

115. As a result of Ticketmaster's breach, Plaintiffs and Class Members have suffered actual damages resulting from theft of their PII, as well as the loss of control of their PII, and remain at imminent risk of suffering additional damages in the future.

116. As a result of Ticketmaster's breach, Plaintiffs and the Class Members have suffered actual damages resulting from their attempt to mitigate the effect of the breach of implied contract and subsequent Data Breach, including, but not limited to, taking steps to protect themselves from the loss of their PII. As a result, Plaintiffs and the Class Members have suffered actual identity theft and the ability to control their PII.

117. Accordingly, Plaintiffs and Class Members have been injured as a result of Ticketmaster's breach of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT SIX
BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING

118. Plaintiffs reallege and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

119. Plaintiffs and Class Members entered into and/or were the beneficiaries of contracts with Defendants, as alleged above.

120. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations—both explicit and fairly implied—and would not impair the rights of the other parties to receive their rights, benefits, and reasonable expectations under the contracts. These included the covenants that Defendants would act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' PII and to comply with industry standards and federal and state laws and regulations for the security of this information.

121. Special relationships exist between Defendants and Plaintiffs and Class Members. Defendants entered into special relationships with Plaintiffs and Class Members, who entrusted their confidential PII to Defendants and paid for services with Defendants.

122. Defendants promised and were obligated to protect the confidentiality of Plaintiffs' and Class Members' PII from disclosure to unauthorized third parties. Defendants breached the covenant of good faith and fair dealing by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' PII, which resulted in the Data Breach. Defendants unreasonably interfered with the contract benefits owed to Plaintiffs and Class Members by failing to implement reasonable and adequate security measures consistent with industry standards to protect and limit access to the PII of Plaintiffs and the Class in Defendants' possession.

123. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Defendants, including paying Defendants for services and providing them the confidential PII required by the contracts.

124. As a result of Defendants' breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class Members did not receive the full benefit of their bargain—services with reasonable data privacy—and instead received services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiffs and Class Members have suffered actual damages in an amount equal to the difference in the

value between services with reasonable data privacy that Plaintiffs and Class Members paid for, and the services they received without reasonable data privacy.

125. As a result of Defendants' breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered actual damages resulting from the theft of their PII and remain at imminent risk of suffering additional damages in the future.

126. As a result of Defendants' breach of the implied covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered actual damages resulting from their attempt to ameliorate the effect of the Data Breach, including, but not limited to, taking steps to protect themselves from the loss of their PII.

127. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class Members suffered injury in fact and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendants from its conduct. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law.

COUNT SEVEN
UNJUST ENRICHMENT
(ALTERNATIVE TO BREACH OF CONTRACT CLAIM)

128. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

129. Plaintiffs and Class Members conferred a monetary benefit on Defendants in the form of monetary payments—directly or indirectly—for services received.

130. Defendants collected, maintained, and stored the PII of Plaintiffs and Class Members and, as such, Defendants had knowledge of the monetary benefits conferred by Plaintiffs and Class Members.

131. The money that Plaintiffs and Class Members paid to Defendants should have been used to pay, at least in part, for the administrative costs and implementation of data management and security. Defendants failed to implement—or adequately implement—practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

132. As a result of Defendants' failure to implement security practices, procedures, and programs to secure sensitive PII, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in the value between services with reasonable data privacy that Plaintiffs and Class Members paid for, and the services they received without reasonable data privacy.

133. Under principles of equity and good conscience, Defendants should not be permitted to retain money belonging to Plaintiffs and Class Members because Defendants failed to implement the data management and security measures that are mandated by industry standards and that Plaintiffs and Class Members paid for.

134. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds received by Defendants. A constructive trust should be imposed upon all unlawful and inequitable sums received by Defendants traceable to Plaintiffs and the Class.

COUNT EIGHT
DECLARATORY JUDGMENT

135. Plaintiffs reallege and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

136. Plaintiffs and the Class have stated claims against Defendants based on negligence, negligence per se, gross negligence and negligent misrepresentation, and violations of various state and federal statutes.

137. Defendants failed to fulfill their obligations to provide adequate and reasonable security measures for the PII of Plaintiffs and the Class, as evidenced by the Data Breach.

138. As a result of the Data Breach, Defendants' system is more vulnerable to unauthorized access and requires more stringent measures to be taken to safeguard the PII of Plaintiffs and the Class going forward.

139. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' current obligations to provide reasonable data security measures to protect the PII of Plaintiffs and the Class. Defendants maintain that its security measures were—and still are—

reasonably adequate and denies that they previously had or have any obligation to implement better safeguards to protect the PII of Plaintiffs and the Class.

140. Plaintiffs seek a declaration that Defendants must implement specific additional, prudent industry security practices to provide reasonable protection and security to the PII of Plaintiffs and the Class. Specifically, Plaintiffs and the Class seek a declaration that Defendants' existing security measures do not comply with their obligations, and that Defendants must implement and maintain reasonable security measures on behalf of Plaintiffs and the Class to comply with their data security obligations.

B. Claims Brought on Behalf of the California Subclass

COUNT NINE
VIOLATION OF THE
CALIFORNIA CUSTOMER RECORDS ACT,
CAL. CIV. CODE §§ 1798.80, *ET SEQ.*

141. Plaintiff Curry ("Plaintiff" for purposes of this claim), individually and on behalf of the California Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach.

142. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

143. Defendants are businesses that own, maintain, and license "personal information", within the meaning of Cal. Civ. Code § 1798.81.5(d)(1), about Plaintiffs and California Subclass members.

144. On information and belief, Live Nation and/or Ticketmaster is registered as a "data broker" in California, which is defined as a "business that knowingly collects and sells to

third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80.[19]

145. Businesses that own or license computerized data that includes personal information, including SSNs, are required to notify California residents when their personal information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

146. Defendants are businesses that own or license computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82(h).

147. Plaintiff and California Subclass members' Private Information includes "personal information" as covered by Cal. Civ. Code §§ 1798.81.5(d)(1), 1798.82(h).

148. Because Defendants reasonably believed that Plaintiff and California Subclass members' Private Information was acquired by unauthorized persons during the Data Breach, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

149. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Cal. Civ. Code § 1798.82.

150. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above.

151. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

[19] https://oag.ca.gov/data-broker/registration/185724.

COUNT TEN
VIOLATION OF THE
CALIFORNIA UNFAIR COMPETITION LAW,
CAL. BUS. & PROF. CODE §§ 17200, *ET SEQ.*

152. Plaintiff Curry ("Plaintiff" for purposes of this claim), individually and on behalf of the California Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach.

153. Defendants are each a "person" as defined by Cal. Bus. & Prof. Code §17201.

154. Defendants violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

155. Defendants' "unfair" and "deceptive" acts and practices include:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and the California Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f) Failing to timely and adequately notify Plaintiff and the California Subclass Members of the Data Breach;

g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and the California Subclass Members' Private Information; and

h) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

156. Defendants have engaged in "unlawful" business practices by violating multiple laws, including the CCRA, Cal. Civ. Code §§ 1798.80, *et seq.*, the CLRA, Cal. Civ. Code §§ 1780, *et seq.*, 15 U.S.C. § 680, *et seq.,* the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

157. Defendants' unlawful practices include:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq*., HIPAA, 42 U.S.C. § 1320d., COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the Data Breach;

d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and the California Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq*., HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501- 6505, and the CMIA, Cal. Civ. Code § 56.36(b);

f) Failing to timely and adequately notify the Plaintiff and the California Subclass Members of the Data Breach;

g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and the California Subclass Members' Private Information; and

h) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq*., HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

158. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

159. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the California Subclass members, into believing that their Private Information was secure.

160. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or

property, including monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information, including, but not limited to, the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

161. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff and California Subclass members' rights.

162. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT ELEVEN
VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT, CAL. CIV. CODE §§ 1750, *ET SEQ.*

163. Plaintiff Curry ("Plaintiff" for purposes of this claim), individually and on behalf of the California Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach.

164. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

165. Defendants are each a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

166. Plaintiff and the California Subclass are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

167. Defendants' acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including:

a) Representing that goods or services have characteristics that they do not have;

b) Representing that goods or services are of a particular standard, quality, or grade when they were not;

c) Advertising goods or services with intent not to sell them as advertised; and

d) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

168. Defendants violated Civil Code § 1770, in the following ways:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d., COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the Data Breach;

d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501- 6505, and the CMIA, Cal. Civ. Code § 56.36(b);

f) Failing to timely and adequately notify the Plaintiff and California Subclass members of the Data Breach;

g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

169. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

170. Had Defendants disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants were trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff, the Class, and the California Subclass. Defendants accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Defendants held itself out as maintaining a secure platform for Private Information data, Plaintiff, the Class, and the California Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

171. As a direct and proximate result of Defendants' violations of California Civil Code § 1770, Plaintiff and California Subclass members have suffered and will continue to

suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, including but not limited to the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

172. Plaintiff and the California Subclass seek an order enjoining the acts and practices described above.

COUNT TWELVE
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT, CAL. CIV. CODE §§ 1798.100, *ET SEQ.*

173. Plaintiff Curry ("Plaintiff" for purposes of this claim), individually and on behalf of the California Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach.

174. Plaintiff and California Subclass members are residents of California.

175. Defendants are corporations that are organized or operated for the profit or financial benefit of its shareholders or other owners. Live Nation had annual gross revenue over $22.7 billion in 2023.

176. Defendants are each a business that collects consumers' personal information as defined by Cal. Civ. Code § 1798.140(e). Specifically, Defendants obtain, receive, or access consumers' personal information when customers sign up for Defendants service.

177. On information and belief, Defendants are each registered as a "data broker" in California, which is defined as a "business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80.

178. Defendants violated Section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiff and the California Subclass members' nonencrypted and nonredacted

personal information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

179. Defendants knew or should have known that its data security practices were inadequate to secure the California Subclass members' Private Information and that its inadequate data security practices gave rise to the risk of a data breach.

180. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the Private Information they collected and stored.

181. The cybercriminals accessed "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d), in the Data Breach.

182. Upon information and belief, Plaintiff and California Subclass members' Private Information accessed by the cybercriminals in the Data Breach includes "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d).

183. Plaintiff seeks injunctive relief in the form of an order requiring Defendants to employ adequate security practices consistent with law and industry standards to protect the California Subclass members' Private Information, requiring Defendants to complete its investigation, and to issue an amended statement giving a detailed explanation that confirms, with reasonable certainty, what categories of data were stolen and accessed without the California Subclass members' authorization, along with an explanation of how the data breach occurred.

184. Plaintiff and the California Subclass members seek statutory damages or actual damages, whichever is greater, pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

185. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §§ 1798.150, Plaintiff and California Subclass members suffered damages, as described above.

186. Plaintiff and the California Subclass seek pecuniary damages pursuant to Cal. Civil Code § 1798.150(b).

C. Claims Brought on Behalf of the Illinois Subclass

COUNT THIRTEEN
VIOLATION OF THE
ILLINOIS CONSUMER FRAUD ACT,
815 ILL. COMP. STAT. §§ 505, ET *SEQ.*

187. Plaintiff Freifeld, individually and on behalf of the Illinois Subclass, incorporate all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of Illinois and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach.

188. Defendants are each a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

189. Plaintiff and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

190. Defendants' conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

191. Defendants' deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b) Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Illinois Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Illinois Subclass Members' PII; and

g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

192. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

193. Defendants intended to mislead Plaintiff and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

194. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

195. Defendants acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois Subclass Members' rights.

196. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to one or more of the following: (i) ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (ii) actual identity theft crimes, fraud, and other

misuse, resulting in monetary loss and economic harm; (iii) loss of the value of their privacy and the confidentiality of the stolen PII; (iv) illegal sale of the compromised PII on the black market; (v) mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (vi) time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; (vii) expenses and time spent initiating fraud alerts; (viii) decreased credit scores and ratings; (ix) lost work time; (x) lost value of PII; (xi) lost value of access to PII permitted by Defendants; (xii) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendants' Data Breach; (xiii) lost benefits of bargains as well as overcharges for services or products; (xiv) nominal and general damages; and (xv) other economic and non- economic harm.

197. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT FOURTEEN
VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 ILL. COMP. STAT. §§ 510/2, *ET SEQ.*

198. Plaintiff Freifeld, individually and on behalf of the Illinois Subclass, incorporate all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of Illinois and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach.

199. Defendants are each a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

200. Defendants engaged in deceptive trade practices in the conduct of their business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a) Representing that goods or services have characteristics that they do not have;

b) Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c) Advertising goods or services with intent not to sell them as advertised; and

d) Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

201. Defendants' deceptive acts and practices include:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b) Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Illinois Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Illinois Subclass Members' PII; and

g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

202. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

203. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

204. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to one or more of the following: (i) ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (ii) actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (iii) loss of the value of their privacy and the confidentiality of the stolen PII; (iv) illegal sale of the compromised PII on the black market; (v) mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (vi) time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; (vii) expenses and time spent initiating fraud alerts; (viii) decreased credit scores and ratings; (ix) lost work time; (x) lost value of PII; (xi) lost value of access to PII permitted by Defendants; (xii) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendants' Data Breach; (xiii) lost benefits of bargains as well as overcharges for services or products; (xiv) nominal and general damages; and (xv) other economic and non- economic harm.

205. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

VII. PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and on behalf of the proposed Class and Subclass, request that the Court:

a. Certify this case as a class action, appoint Plaintiffs as class representatives, and appoint Plaintiffs' Counsel as Class Counsel for Plaintiffs to represent the Class;

b. Find that Defendants breached its duty to safeguard and protect the PII of Plaintiffs and Class Members that was compromised in the Data Breach;

c. Award Plaintiffs and Class Members appropriate relief, including actual and statutory damages, restitution and disgorgement;

d. Award equitable, injunctive and declaratory relief as may be appropriate;

e. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

f. Award pre-judgment and post-judgment interest as prescribed by law; and

g. Grant additional legal or equitable relief as this Court may find just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated June 7, 2024

Respectfully submitted,

COTCHETT PITRE & MCCARTHY LLP

/s/ Thomas E. Loeser
Thomas E. Loeser (*SBN: 202724*)
Karin B. Swope (*pro hac vice to be filed)*
999 N. Northlake Way, Suite 215
Seattle, WA 98103
Tel: (206) 802-1272
Fax: (650) 697-0577
tloeser@cpmlegal.com.com

Attorneys for Plaintiffs James Curry and David Freifeld the proposed Class