Jennifer M. French, State Bar No. 265422
LYNCH CARPENTER, LLP
1234 Camino Del Mar
Del Mar, CA 92014
Tel: (619) 762-1910
Fax: (858) 313-1850
jennf@lcllp.com

Gary F. Lynch*
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Floor
Pittsburgh, PA 15222
Tel.: (412) 322-9243
Fax: (724) 656-1556
gary@lcllp.com

Attorneys for Plaintiff and the Class

**Pro hac vice forthcoming*

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MATTHEW MILLER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

TICKETMASTER, LLC; and LIVE NATION ENTERTAINMENT, INC.,

Defendants.

Case No. 2:24-cv-5867

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Matthew Miller, individually and on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against Defendants Ticketmaster, LLC and Live Nation Entertainment, Inc. Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

NATURE OF THE ACTION

1. Plaintiff brings this action against Defendants for their failure to properly secure and safeguard highly valuable, protected, personally identifiable information including customer names, email addresses, phone numbers, and credit card details (collectively, "PII") and for their failure to comply with industry standards to protect information systems that contain PII.

2. Ticketmaster is one of the largest ticket sales and distribution companies in the world. Upon information and belief, in 2009, Ticketmaster entered into an agreement to merge with event promoter and venue operator Live Nation to form Live Nation Entertainment, Incorporated. Together, Defendants promote, operate, and manage entertainment venues and ticket sales for live entertainment events.

3. Defendants operate a digital ticketing platform that requires customers to provide their PII in order to make a purchase. To make a purchase from Defendants, customers are required to entrust Defendants with their PII and, in return, reasonably expect that Defendants will safeguard that PII.

4. As large entertainment companies who engage in the sale and distribution of event tickets, Defendants knowingly collect and store sensitive customer PII and have a resulting duty to secure this information from unauthorized access and exfiltration.

/ / /

/ / /

5. Defendants expressly recognize their duty to safeguard customer PII, stating: "We have security measures in place to protect your information."[1]

6. Despite their duties to safeguard customer PII, however, on or about 31 May 2024, Defendants confirmed that customer PII had been stolen from Defendants' third-party cloud database provider by threat actors (the "Data Breach").[2]

7. The information stolen during the Data Breach included databases containing 1.3 terabytes of data, including the PII of approximately 560 million Ticketmaster customers. The cybercriminals who claimed responsibility for the Data Breach then proceeded to advertise the stolen customer PII for sale on their dark web leak site for $500,000.[3]

8. As a direct and proximate result of Defendants' failure to implement and follow basic security procedures, Plaintiff and Class (defined below) members' PII—names, email addresses, phone numbers, and credit card details—is now in the hands of cybercriminals and offered for sale on the dark web.

9. Plaintiff and Class members are now at a significantly increased and impending risk of fraud, identity theft, and other harms caused by the unauthorized disclosure of their PII—risks that may last for the rest of their lives. Consequently, Plaintiff and Class members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

---

[1] Live Nation Help, *Live Nation Entertainment Privacy Policy* (Dec. 1, 2022), https://help.livenation.com/hc/en-us/articles/10464047306641-Live-Nation-Entertainment-Privacy-Policy.

[2] Lawrence Abrams, *Ticketmaster Confirms Massive Breach After Stolen Data for Sale* Online, Bleeping Computer (May 31, 2024), https://www.bleepingcomputer.com/news/security/ticketmaster-confirms-massive-breach-after-stolen-data-for-sale-online/.

[3] Sergiu Gatlan, *Data of 560 Million Ticketmaster Customers for Sale After Alleged Breach*, Bleeping Computer (May 30, 2024), https://www.bleepingcomputer.com/news/security/data-of-560-million-ticketmaster-customers-for-sale-after-alleged-breach/.

10. As such, on behalf of himself and all others similarly situated, Plaintiff brings claims for negligence, negligence per se, breach of implied contract, unjust enrichment, and declaratory judgment, seeking damages and injunctive relief, including the adoption of reasonably sufficient data security practices to safeguard the PII in Defendants' possession to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

11. Plaintiff Matthew Miller is an adult who, at all relevant times, is and was citizen of the State of Utah. Plaintiff received a Data Breach letter from Ticketmaster informing him that the PII he entrusted to Defendants was compromised in the Data Breach.

12. Defendant Live Nation is a Delaware corporation with a principal place of business located at 9348 Civic Center Drive, Beverly Hills, CA 90210.

13. Defendant Ticketmaster is a Virginia limited liability company with a principal place of business located at 9348 Civic Center Drive, Beverly Hills, CA 90210. Upon information and belief, Ticketmaster is a single member limited liability company, with its sole member being Live Nation Worldwide, Inc, a Delaware corporation with a principal place of business located at 9348 Civic Center Drive, Beverly Hills, CA 90210. Ticketmaster is a citizen of each State in which its member is a citizen. Ticketmaster is therefore a citizen of the States of Delaware and California.

JURISDICTION AND VENUE

14. This Court has jurisdiction over this action under 28 U.S.C. § 1332(d), the Class Action Fairness Act, because Plaintiff and at least one member of the Class, as defined below, are citizens of a different state than Defendants, there are more than 100 members in the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs.

/ / /

15. This Court has general personal jurisdiction over Defendants because Defendants reside in the State of California and regularly sell and offer to sell products and services in the State of California.

16. This Court is the proper venue for this action under 28 U.S.C. § 1391(b)(1), because Defendants reside in this District, a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District, and Defendants conduct substantial business within this District.

FACTUAL BACKGROUND

A. Defendants' Collect and Store Highly Valuable Customer PII

17. Defendants promote, operate, and manage entertainment venues and ticket sales for live entertainment events. To promote and sell tickets for live entertainment events, Defendants operate the website www.ticketmaster.com, which allows Defendants' customers to buy and sell tickets for concerts, sports, theater, and other live entertainment events.

18. To buy and sell tickets on Defendants' online platform, Plaintiff and Class members are required to entrust Defendants with their PII, including names, email addresses, phone numbers, and credit card details.

19. Upon information and belief, Defendants ultimately store their customers' PII in a third-party cloud database.

20. When collecting and storing customer PII, Defendants promised to provide Plaintiff and Class members with adequate data security measures to protect their PII. Specifically, when customer data is transferred to third parties, such as the third-party cloud database provider Defendants engage to store customers PII, Defendants promised "ensure that appropriate safeguards are put in place" to ensure customer data is "protected to the highest standard."[4] Defendants further represented that they would "use contractual measures and

[4] Ticket Master, *Privacy Policy*, https://privacy.ticketmaster.com/privacy-policy (last visited Jul. 11, 2024).

internal mechanisms requiring the recipient to comply with the privacy standards of the exporter."[5]

21. Plaintiff and Class members relied on these representations and reasonably expected that, when they provided their PII to Defendants, Defendants would employ adequate data security measures to protect customer PII.

22. Despite Defendants' stated commitment to data security, however, Defendants failed to adopt reasonable measures to prevent the unauthorized access to Plaintiff's and Class members' PII by bad actors.

B. The Data Breach

23. On or about 30 May 2024, news outlets began reporting that a threat actor was selling what was alleged to be the personal and financial information of 560 million Ticketmaster customers.[6] The threat actor demanded $500,000 for the sale of the stolen customer information.[7]

24. The threat actor put the alleged stolen databases for sale on a hacking forum and represented that the databases contained 1.3 terabytes of customer PII, including names, email addresses, and credit card details. The information appeared to relate to financial transactions spanning from 2012 to 2024.[8]

25. The next day, Defendants confirmed that they had suffered a data breach, indicating that the stolen data offered for sale on the dark web was customer PII stolen from a third-party cloud database provider. Defendants further confirmed that they had identified unauthorized access in that cloud database on or about 20 May 2024.[9]

/ / /

[5] *Id.*
[6] Gatlan, *supra* note 3.
[7] *Id.*
[8] *Id.*
[9] Abrams, *supra* note 2.

26. On or about 28 June 2024, Defendants began notifying impacted individuals of the Data Breach, indicating that the threat actor had gained unauthorized access to the cloud database between 2 April 2024 and 18 May 2024.[10]

27. Since Defendant' confirmation of the Data Breach, the threat actors have increased their extortion attempts, leaking what they claim to have been Ticketmaster barcode data for 166,000 tickets from the extremely popular Taylor Swift Eras Tour. The threat actors further demanded $2 million or else they would leak 30 million additional event barcodes, including barcodes to Taylor Swift, P!nk, Sting, and sporting events.[11]

28. Later, threat actors leaked nearly 39,000 Ticketmaster print-at home tickets for 154 upcoming concerts and events, including Pearl Jam, Phish, Tate McCrae, and Foo Fighters.[12]

29. Security researchers reported that the Data Breach is the result of threat actors gaining access to Defendants' third-party cloud databases via compromised login credentials. It appears the login credentials were stolen via historical infostealer malware infections.[13]

30. Security researchers also reported that access to the cloud storage databases is the result of "because of poor security practices on impacted accounts,

[10] Ticketmaster LLC, *Submitted Breach Notification Sample*, Cal. Dept. of Justice, https://oag.ca.gov/system/files/%5BT01%5D%20US-General.pdf (last visited Jul. 11, 2024).

[11] Lawrence Abrams, *Hackers Leak Alleged Taylor Swift Tickets, Amp Up Ticketmaster Extortion*, Bleeping Computer (Jul. 5, 2024), https://www.bleepingcomputer.com/news/security/hackers-leak-alleged-taylor-swift-tickets-amp-up-ticketmaster-extortion/.

[12] Lawrence Abrams, *Hackers Leak 39,000 Print-at-Home Ticketmaster Tickets for 154 Events*, Bleeping Computer (Jul. 8, 2024), https://www.bleepingcomputer.com/news/security/hackers-leak-39-000-print-at-home-ticketmaster-tickets-for-154-events/.

[13] Jess Weatherbed, *Ticketmaster's Snowflake Data Breach Was Just One of 165*, The Verge (Jun. 11, 2024), https://www.theverge.com/2024/6/11/24176080/snowflake-cloud-storage-data-breach-ticketmaster-santander.

which did not update stolen login credentials or utilize multi-factor authentication (MFA) or network allow lists."[14]

31. Upon information and belief, the Data Breach occurred as a direct and proximate result of Defendants' failure to implement and follow basic security procedures to protect customers' PII, including regularly updating login credentials for their third-party cloud storage databases and/or enabling MFA for access to those cloud storage databases.

C. The Value of PII and Effects of Unauthorized Disclosure

32. Defendants understood the protected PII that they acquire is highly sensitive and of significant value to those who would use it for wrongful, nefarious purposes.

33. Defendants also knew that a breach of their computer systems or databases, and exposure of the PII therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

34. These risks are not theoretical; numerous high-profile breaches have occurred as a result of compromised cloud storage platforms in recent years, including CapitalOne.

35. PII is a valuable commodity to identity thieves. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[15] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the dark web.

/ / /

/ / /

[14] *Id.*

[15] Fed. Trade Comm'n Consumer Advice, *What To Know About Identity Theft* (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

36. Criminals often trade stolen PII on the cyber black market for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available.

37. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[16]

38. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[17]

39. Cloud storage databases are prime targets for cybercriminals. It is estimated that more than 60% of the world's corporate data is stored in the cloud, making the cloud a highly attractive target for cybercriminals.[18]

40. Indeed, "[i]n 2023, over 80% of data breaches involved data stored in the cloud. That is not just because the cloud is an attractive target. In many cases, it is also an easy target due to cloud misconfiguration – that is, companies unintentionally misuse the cloud, such as allowing excessively permissive cloud access, having unrestricted ports, and use unsecured backups."[19]

/ / /

[16] *New Report from Flashpoint and Risk Based Security Finds 22 Billion Records Exposed in 2021 Data Breaches*, Flashpoint (Feb. 4, 2022), https://flashpoint.io/blog/2021-data-breach-report/.

[17] *Facts + Statistics: Identity Theft and Cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Jul. 11, 2024).

[18] Stuart Madnick, *Why Data Breaches Spiked in 2023*, Harvard Business Review (Feb. 19, 2024), https://hbr.org/2024/02/why-data-breaches-spiked-in-2023.

[19] *Id.*

41. According to the National Security Agency, "'cloud misconfigurations are the most prevalent cloud vulnerability' and can be exploited by hackers to access cloud data and services."[20]

42. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class members especially vulnerable to identity theft, tax fraud, credit and bank fraud, and more.

43. Cybercriminals can use stolen payment card information to create counterfeit payment cards and make unauthorized charges or withdrawals that can cause consumers to incur significant financial losses. Indeed, the counterfeit payment cards (or the compromised payment card information itself) can be used to purchase high-ticket goods or gift cards that can then be sold for cash all while charging the consumer's original card. Cybercriminals can also sell the stolen payment card information to other cybercriminals on the dark web. In turn, when a payment card is fraudulently used, it can damage the cardholder's credit score, making it difficult to obtain new credit in the future.

44. Even if stolen PII does not include financial or payment card account information, it does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Indeed, even where cybercriminals do not gain access to a complete set of an individual's PII during a data breach, cybercriminals can cross-reference two or more sources of PII to marry data available elsewhere with criminally stolen data, resulting in complete and accurate dossiers on individuals. These dossiers are known as "Fullz" packages.

45. The development of Fullz packages means stolen PII from a data breach can easily be linked to victims' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain

[20] *Id.*

information (such as emails, phone numbers, or credit card numbers) is not included in the PII stolen in a specific incident, criminals can easily create a Fullz package that links that information together and sell the package at a higher price.

46. Importantly, once a cybercriminal has a Fullz package, they can use it to commit a host of criminal acts including: credit card fraud, loan fraud, identity fraud, account take overs, medical identity fraud, tax refund fraud, and buy now pay later frauds.[21] Most problematic, however, is that cybercriminals in possession of a Fullz package "are difficult to stop with ordinary online security and ID verification measures because they possess all the information needed to get past typical authentication measures."[22]

47. A poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[23]

48. Due to high-profile data breaches at other companies, Defendants knew or should have known that their computer systems and cloud storage databases would be targeted by cybercriminals.

49. Defendants also knew or should have known the importance of safeguarding the PII with which they were entrusted and of the foreseeable consequences if their data security systems were breached. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach and the exfiltration of its customers' PII from occurring.

---

[21] Paige Tester, *What Are Fullz? How Hackers and Fraudsters Obtain and Use Fullz*, DataDome (Mar. 3, 2024), https://datadome.co/guides/account-takeover/what-are-fullz-how-do-fullz-work/.

[22] *Protection Against Fullz and Fraud*, Integrity (Apr. 18, 2022), https://integrity.aristotle.com/2022/04/protection-against-fullz-and-fraud/.

[23] Chuck Brooks, *Alarming Cyber Statistics for Mid-Year 2022 That You Need to Know*, Forbes (Jun. 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/.

D. Defendants Failed to Comply with FTC Guidelines and Industry Best Practices

50. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an unfair practice in violation of the FTC Act.

51. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[24]

52. The FTC recommends that businesses:

a. identify all connections to the computers where sensitive information is stored;

b. assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

[24] U.S. Federal Trade Comm'n, *Start with Security: A Guide for Business* (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.

e. pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.[25]

53. The FTC further recommends business take additional cybersecurity steps, which include:

[25] U.S. Federal Trade Comm'n, *Protecting Personal Information: A Guide for Business*, (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

a. conducting an inventory of all company devices that store sensitive data, and understanding what types of PII is stored on those devices;

b. encrypting sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. crafting a data security plan that involves both physical security (*e.g.*, locking up physical files) and electronic security, and training employees regarding the data security plan.

d. promptly disposing of PII that is no longer needed, and retaining sensitive data only as long as companies maintain a legitimate business need for the information; and

e. developing a plan to handle a data breach or data security incident, if and when such an incident occurs.[26]

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

55. Upon information and belief, Defendants failed to properly implement one or more of the basic data security practices described above. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII resulted in the unauthorized access to and exfiltration of Plaintiff and Class members' PII.

/ / /

/ / /

[26] *Id.*

56. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

57. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[27]

58. The NIST's publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[28] Upon information and belief, Defendants failed to adhere to the NIST guidance.

59. Further, there are various best practices that should be implemented by entities who use cloud storage databases, including the following:

a. implementing strong passwords, multifactor authentication, and data encryption;

b. analyzing system logs on a regular basis to identity unexpected login attempts or other suspicious activities;

c. providing employees with training on data security best practices and what steps the can take to safeguard company data;

d. conducting regular security assessments, including security audits, penetration testing, and vulnerability assessments; and

e. keeping software up-to-date with security updates and fixes.[29]

[27] *See* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* app. A, tbl. 2, (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.
[28] *Id.* at tbl. 2, pp. 26–43.
[29] *Top 12 Cloud Security Breaches in* History, Blue Bird Int'l (Jan. 28, 2023), https://bluebirdinternational.com/top-12-cloud-security-breaches/.

60. Upon information and belief, Defendants' failure to protect Plaintiff and Class members' PII is a result of Defendants' failure to adopt reasonable safeguards required by the FTC, NIST, and industry best practices.

61. Defendants were, at all times, fully aware of their obligations to protect the PII of consumers because of their business model of collecting and storing PII. Defendants were also aware of the significant repercussions that would result from their failure to do so.

D. Plaintiff and Class Members Suffered Damages

62. The ramifications of Defendants' failure to keep consumers' PII secure are long-lasting and severe. Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class members significant injuries and harm in several ways, including theft of their PII as well as substantial and imminent risk of identity theft and fraud. Plaintiff and Class members must immediately devote time, energy, and money to: (1) closely monitor their bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering, spear phishing, or extortion attacks; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

63. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps consumers can take after a data breach.[30] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the

[30] U.S. Gov't Accountability Off., *Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services* (Mar. 2019), https://www.gao.gov/assets/gao-19-230.pdf.

steps data breach victims (like Plaintiff and Class members) must take after a data breach like this one are both time-consuming and of only limited and short-term effectiveness.

64. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[31]

65. Defendants themselves recognize the certainly impending and increased risk of identity theft and fraud that Plaintiff and Class members now face as they have provided individuals impacted by the Data Breach one year of identity protection services.[32] Defendants further recommended Plaintiff and Class members "remain vigilant and take steps to protect against identity theft and fraud, including monitoring your accounts, account statements, and credit reports for signs of suspicious activities."[33]

66. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse.

67. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered and between when PII is stolen and when it is used. According to the GAO, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on

[31] *See* U.S. Fed. Trade Comm'n, *Identity Theft Victim Checklist* https://www.identitytheft.gov/Steps (last accessed Jul. 11, 2024).
[32] *Submitted Breach Notification Sample*, *supra* note 11.
[33] *Id.*

> the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[34]

68. For these reasons, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives, because of Defendants' conduct.

69. The value of Plaintiff and Class members' PII has been diminished by its exposure in the Data Breach. PII is a valuable commodity to identity thieves, and, once it has been compromised, criminals will use and trade the information on the cyber black market for years thereafter.[35]

70. The reality is that cybercriminals seek nefarious outcomes from a data breach, and stolen PII can be used to carry out a variety of crimes.

71. Plaintiff and Class members are also at a continued risk because their information remains in Defendants' systems and/or cloud storage databases, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect their customers' PII.

72. As a result of Defendants' failures, Plaintiff and Class members face an increased risk of identity theft and fraud, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

73. Plaintiff and Class members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud,

[34] *See* U.S. Gov't Accountability Off., *Personal Information* 29 (Jun. 2007), available at https://www.gao.gov/assets/gao-07-737.pdf.

[35] *The Price Cybercriminals Charge for Stolen Data*, Trustwave SpiderLabs (Aug. 3, 2022), https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-price-cybercriminals-charge-for-stolen-data/.

and the unauthorized exposure of their private information to strangers and cybercriminals.

E. Plaintiff's Experience

74. Plaintiff is a Ticketmaster customer. To buy and sell tickets on Defendants' platform, Plaintiff was required to entrust Defendants with his PII, and he reasonably expected that Defendants would implement reasonable data security measures to safeguard his PII from unauthorized access and exfiltration.

75. On 2 July 2024, Plaintiff received a data breach notification from Defendants informing him that the PII he entrusted to Defendants was compromised in the Data Breach.

76. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time and effort taking steps to mitigate the risk of misuse of his PII, including monitoring his credit card statements for suspicious activity. Plaintiff would not have had to engage in these time intensive efforts but for the Data Breach.

77. Since the announcement of the Data Breach, Plaintiff has also seen an increase in the number of spam calls and emails he receives. Plaintiff noticed that this is a substantial increase in the amount spam he has received, as opposed the amount of spam he received before the Data Breach.

78. Plaintiff has suffered actual injury from having his PII exposed and/or stolen as a result of the Data Breach, including: (a) mitigation efforts to prevent the misuse of his PII; (b) damages to and diminution of the value of his PII, a form of intangible property that loses value when it falls into the hands of criminals who use that information for fraud or publish the information for sale on the dark web; and (c) loss of privacy.

79. Given the nature of the information compromised in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff faces a significant, present, and ongoing risk of

identity theft and fraud, and other identity-related fraud now and into the indefinite future.

80. In addition, knowing that hackers accessed and likely exfiltrated his PII and that this information likely has been and will be used in the future for identity theft, fraud, and other nefarious purposes has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

CLASS ACTION ALLEGATIONS

81. Plaintiff brings this case individually and under Rule 23 of the Federal Rules of Civil Procedure on behalf of the class defined as:

> All individuals in the United States whose PII was compromised in the Data Breach that was confirmed by Defendants on or about 31 May 2024 (the "Class").

82. Excluded from the Class are Defendants, their subsidiaries and affiliates, their officers, directors, and members of their officers' and directors' immediate families, any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of those judicial officers' immediate families.

83. Plaintiff reserves the right to modify or amend the definition of the proposed Class before moving for class certification.

84. **Numerosity.** The putative Class is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendants' records, including, but not limited to, the files implicated in the Data Breach. Upon information and belief, the Class includes at least 560 million individuals.

85. **Commonality.** This action involves questions of law and fact that are common to Plaintiff and the Class members. Such common questions include, but are not limited to:

a. whether and to what extent Defendants had a duty to protect the PII of Plaintiff and Class members;

b. whether Defendants were negligent in collecting and storing Plaintiff and Class members' PII;

c. whether Defendants had duties not to disclose Plaintiff and Class members' PII to unauthorized third parties;

d. whether Defendants took reasonable steps and measures to safeguard Plaintiff and Class members' PII;

e. whether Defendants failed to adequately safeguard Plaintiff and Class members' PII;

f. whether Defendants breached their duties to exercise reasonable care in handling Plaintiff and Class members' PII;

g. whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. whether Plaintiff and Class members are entitled to damages as a result of Defendants' wrongful conduct; and

i. whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

86. **Typicality.** Plaintiff's claims are typical of the claims of the Class members. The claims of Plaintiff and Class members are based on the same legal theories and arise from the same failure by Defendants to safeguard their PII. Plaintiff and Class members entrusted Defendants with their PII, and it was subsequently accessed by an unauthorized third party.

87. **Adequacy of Representation.** Plaintiff is adequate representative of the Class because his interests do not conflict with the interests of the other Class members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

88. **Superiority.** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

89. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached their duties and released Plaintiff and Class members' PII, then Plaintiff and each Class member suffered damages by that conduct.

90. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class members may be readily identified through Defendants' books and records.

/ / /

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)
(Against all Defendants)

91. Plaintiff restates and realleges all proceeding allegations as if fully set forth herein.

92. Defendants owed a duty under common law to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

93. Specifically, this duty included, among other things: (a) maintaining and testing Defendants' security systems to ensure that Plaintiff and Class members' PII in Defendants' possession was adequately secured and protected; (b) implementing processes that would detect a breach of Defendants' security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

94. Defendants' duty to use reasonable care arose from several sources, including, but not limited to, those described below.

95. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

96. Defendants also owed a common law duty because their conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendants'

conduct included their failure to adequately restrict access to their computer networks and/or cloud databases that held individuals' PII.

97. Defendants also knew or should have known of the inherent risk in collecting and storing massive amounts of PII, the importance of implementing adequate data security measures to protect that PII, and the frequency of cyberattacks like the Data Breach that target cloud storage database.

98. Defendants breached the duties owed to Plaintiff and Class members and thus were negligent. Defendants breached these duties by, among other things: (a) mismanaging their systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies provided to customers; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

99. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class members, their PII would not have been accessed, exfiltrated, and compromised by cybercriminals.

100. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have suffered injuries including:

a. theft of their PII;

b. unauthorized charges to their bank accounts;

c. costs associated with canceling and ordering new payment cards;

d. time spent reporting fraudulent activity;

e. costs associated with requesting credit freezes;

f. costs associated with the detection and prevention of identity theft;

g. costs associated with purchasing credit monitoring and identity theft protection services;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach;

j. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

k. damages to and diminution in value of their PII entrusted to Defendants with the mutual understanding that Defendants would safeguard Plaintiff and Class members' data against theft and not allow access and misuse of their data by others; and

l. continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff and Class members.

101. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

/ / /

SECOND CAUSE OF ACTION

NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)
(Against all Defendants)

102. Plaintiff restates and realleges all proceeding factual allegations as if fully set forth herein.

103. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendants for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

104. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of a data breach.

105. Defendants' violation of Section 5 of the FTC Act constitutes negligence per se.

106. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

107. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

108. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have suffered injuries, including those identified in paragraph 100 above.

109. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)
(Against all Defendants)

110. Plaintiff restates and realleges all proceeding factual allegations as if fully set forth herein.

111. As a condition of using Defendants' platform to buy and sell tickets, Defendants required Plaintiff and Class members to directly or indirectly entrust them with their PII.

112. As a result of these transactions, Plaintiff and Class members entered implied contracts with Defendants by which Defendants agreed to safeguard and protect such PII and keep such PII secure and confidential from unauthorized access.

113. When entering these implied contracts, Plaintiff and Class members reasonably believed and expected that Defendants' data security practices complied with its statutory and common law duties to adequately protect Plaintiff and Class members' PII.

114. Indeed, implicit in these exchanges was a promise by Defendants to ensure the PII of Plaintiff and Class members in their possession would be used to provide the agreed-upon services and that Defendants would take adequate measures to protect Plaintiff and Class members' PII.

115. It is clear by these exchanges that the parties intended to enter into implied agreements supported by mutual assent. Plaintiff and Class members would not have disclosed their PII to Defendants but for the prospect of Defendants' promise of services. Conversely, Defendants presumably would not

have taken Plaintiff and Class members' PII if not for the intent to provide Plaintiff and Class members with their services.

116. Plaintiff and Class members would not have provided their PII to Defendants had they known that Defendants would not safeguard their PII as promised.

117. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendants.

118. Defendants breached their implied contracts with Plaintiff and Class members by failing to safeguard Plaintiff and Class members' PII.

119. As a direct and proximate result of Defendants' breach of contract, Plaintiff and Class members have suffered injuries, including those identified in paragraph 100 above and the loss of the benefit of their bargains.

120. As a direct and proximate result of Defendants' breach of implied contract, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION

UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)
(Against all Defendants)

121. Plaintiff restates and realleges all proceeding factual allegations as if fully set forth herein.

122. Plaintiff brings this claim in the alternative to his Breach of Implied Contract claim above.

123. Plaintiff and Class members conferred a monetary benefit on Defendants by providing them with their valuable PII.

124. Defendants knew that Plaintiff and Class members conferred a benefit upon them and accepted and retained that benefit by accepting and

retaining the PII entrusted to them. Defendants profited from Plaintiff and Class members' PII and use of Plaintiff and Class members' PII for business purposes.

125. Defendants failed to secure Plaintiff and Class members' PII and, therefore, did not fully compensate Plaintiff or Class members for the value that their PII provided.

126. Defendants acquired the PII through inequitable record retention as Defendants failed to disclose the inadequate data security practices previously alleged.

127. If Plaintiff and Class members had known Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have agreed to the entrustment of their PII to Defendants.

128. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class members conferred upon Defendants.

129. Plaintiff and Class members are without an adequate remedy at law.

130. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have suffered injuries, including those identified in paragraph 100 above.

131. Plaintiff and Class members are entitled to restitution and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct, as well as return of their sensitive PII and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class members may seek restitution or compensation.

/ / /

/ / /

/ / /

FIFTH CAUSE OF ACTION

DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)
(Against all Defendants)

132. Plaintiff restates and realleges all proceeding factual allegations as if fully set forth herein.

133. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described herein.

134. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff and Class members' PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their PII. Plaintiff alleges that Defendants still possess Plaintiff and Class members' PII, and that Defendants' data security measures remain inadequate. Furthermore, Plaintiff and Class members continue to suffer injury as a result of the compromise of their PII and remains at imminent risk that further compromises of their PII will occur in the future.

135. Using its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure consumers' PII under the common law Section 5 of the FTC Act; and

b. Defendants continue to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiff and Class members' PII.

136. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect consumers' PII in their possession.

137. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiff and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

138. The hardship to Plaintiff and Class members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff and Class members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

139. Issuance of the requested injunction will not disserve the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, on behalf of himself and all others similarly situated, prays for relief as follows:

A. for an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. for an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. for damages in an amount to be determined by the trier of fact;

D. for an order of restitution and all other forms of equitable monetary relief;

E. declaratory and injunctive relief as described herein;

F. awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

G. awarding pre- and post-judgment interest on any amounts awarded; and

H. awarding such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

A jury trial is demanded on all claims so triable.

Dated: July 11, 2024

By: */s/ Jennifer M. French*

Jennifer M. French, State Bar No. 265422
LYNCH CARPENTER, LLP
1234 Camino Del Mar
Del Mar, CA 92014
Tel: (619) 762-1910
Fax: (858) 313-1850
jennf@lcllp.com

Gary F. Lynch*
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Floor
Pittsburgh, PA 15222
Tel.: (412) 322-9243
Fax: (724) 656-1556
gary@lcllp.com

Attorneys for Plaintiff and the Class

**Pro hac vice forthcoming*