John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive, Penthouse
Beverly Hills, CA 90212
Tel: (858) 209-6941
jnelson@milberg.com

Counsel for Plaintiff

[Additional counsel listed on signature page]

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CHRISTINA XIAN, on behalf of herself and all others similarly situated, Plaintiff, v. **TICKETMASTER, LLC, and LIVE NATION ENTERTAINMENT, INC.,** Defendants.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Christina Xian ("Plaintiff"), individually and on behalf of all similarly situated persons, allege the following against Ticketmaster, LLC and Live Nation Entertainment, Inc. ("Ticketmaster" or "Live Nation" or collectively "Defendants") based upon personal knowledge with respect to themselves and on

information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Ticketmaster and Live Nation for their failure to properly secure and safeguard Plaintiff's and other similarly situated Ticketmaster customers' names, addresses, phone numbers, and partial credit card details (personal identifying information or "PII") from hackers.

2. Defendant Ticketmaster, LLC is a wholly owned subsidiary of Defendant Live Nation Entertainment, Inc. based in Hollywood, California and is an event ticket selling website that serves more than half a billion event goers and customers in 29 countries.

3. On or about May 31, 2024, Live Nation filed an official report (the "Report") of a hacking incident with the United States Securities and Exchange Commission.

4. The report with the SEC also stated that Defendants have been working with law enforcement, as well as beginning to notify state agencies and impacted customers.

5. Based on the Report filed by the company, on May 20, 2024, Live Nation detected unusual activity on some of its computer systems. In response, the company launched an investigation. The Live Nation investigation revealed that an unauthorized party had access to certain company files (the "Data Breach"). To date, Defendants have yet to notify impacted individuals directly.

6. Plaintiff and "Class Members" (defined below) were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The PII compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, names,

addresses, and payment card information that Ticketmaster collected and maintained.

8. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names and making fraudulent charges on Class Members' impacted payment information.

9. There has been no assurance offered by Defendants that all personal data or copies of data have been recovered or destroyed, or that Defendants have adequately enhanced their data security practices sufficient to avoid a similar breach of their network in the future.

10. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their PII, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiff brings this class action lawsuit to address Defendants' inadequate safeguarding of Class Members' PII that it collected and maintained.

12. The potential for improper disclosure and theft of Plaintiff's and Class Members' PII was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure the PII left it vulnerable to an attack.

13. Upon information and belief, Defendants and their employees failed to properly implement security practices with regard to the computer network and systems that housed the PII. Had Defendants properly monitored their networks, it would have discovered the Breach sooner, or prevented the breach from occurring at all.

14. Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct as the PII that Defendants collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed and/or compromised during the Data Breach.

II. PARTIES

16. Plaintiff Christina Xian is, and at all times mentioned herein was, an individual citizen of the State of California.

17. Defendant Ticketmaster, LLC is a wholly owned subsidiary of Live Nation Entertainment, Inc. and is a limited liability company existing under the laws of Virginia, with its principal place of business in Hollywood, California.

18. Defendant Live Nation Entertainment, Inc. is a ticket and event management company incorporated in Delaware with its principal place of business in Beverly Hills, California.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has personal jurisdiction over Defendants because Defendants operate in and/or are incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Defendants have harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Ticketmaster's Business and Collection of Plaintiff's and Class Members' PII

22. Ticketmaster is a ticket seller and event management company. Founded in 1976, Ticketmaster is the largest ticketing company in the United States, serving more than 500 million customers in all states and internationally. Ticketmaster is a wholly owned subsidiary of Live Nation. Ticketmaster employs more than 6,600 people and generates approximately $16.7 billion in annual revenue.

23. As a condition of receiving ticketing services, Ticketmaster requires that its customers entrust it with highly sensitive personal information. In the ordinary course of receiving service from Ticketmaster, Plaintiff and Class Members were required to provide their PII to Defendants.

24. Ticketmaster uses this information, *inter alia*, to sell, manage, and otherwise promote ticket events.

25. In its privacy policy, Ticketmaster promises its customers that it will keep their information safe, specifically stating that it has "security measures in place to protect your information."[1] Even so, the hacker group "ShinyHunters" was able to steal roughly 1.3TB of customer data, including payment card and other details of approximately 560 million users.[2]

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew

[1] Privacy Policy (ticketmaster.com) (last visited on June 5, 2024).

[2] *See What do we know about the Ticketmaster data breach and the force behind it?, https://time.com/6984811/ticketmaster-data-breach-customers-livenation-everything-to-know/* (last visited on June 5, 2024).

or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure and exfiltration.

27. Plaintiff and Class Members relied on Defendants to keep their PII confidential and securely maintained and to only make authorized disclosures of this information, which Defendants ultimately failed to do.

B. Defendants Failed to Comply with FTC Guidelines

28. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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. Indeed, 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 Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

29. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

30. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a

transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

31. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

32. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

33. Defendants were at all times fully aware of their obligation to protect the PII of their customers yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

C. Defendants Failed to Comply with Industry Standards

34. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

35. Some industry best practices that should be implemented by businesses like Defendants include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and

limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

36. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

37. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

38. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

D. Defendants Breached Their Duty to Safeguard Plaintiff's and Class Members' PII

39. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with industry standards and requirements, training for their staff, and ensuring that their computer systems, networks, and protocols adequately protected the PII of Class Members

40. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' PII;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to sufficiently train their employees regarding the proper handling of their customers PII;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII.

41. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access their computer network and systems which contained unsecured and unencrypted PII.

42. Had Defendants remedied the deficiencies in their information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

43. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and

now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Defendants.

E. Defendants Should Have Known that Cybercriminals Target PII to Carry Out Fraud and Identity Theft

44. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[3] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

45. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

46. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed

[3] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on June 5, 2024).

with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

47. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

48. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' PII to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

49. One such example of this is the development of "Fullz" packages.

50. Cybercriminals can cross-reference two sources of the PII compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

51. The development of "Fullz" packages means that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the

proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the PII stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen PII are being misused, and that such misuse is fairly traceable to the Data Breach.

52. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[4] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

53. Identity thieves can also use stolen personal information such as payment card information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank fraud.

54. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison

[4] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited June 5, 2024).

sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

55. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[5] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants' industry.

56. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[7]

57. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering

---

[5] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on June 5, 2024).

[6] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on June 5, 2024).

[7] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on June 5, 2024).

attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[8]

58. The Dark Web Price Index of 2022, published by PrivacyAffairs[9] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

59. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

60. Likewise, the value of PII is increasingly evident in our digital economy. Many companies, including Defendants, collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[10]

61. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data

---

[8] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on June 5, 2024).

[9] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on June 5, 2024).

[10] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on June 5, 2024).

points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[11]

62. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

63. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

64. An active and robust legitimate marketplace for PII exists. In 2021, the data brokering industry was worth roughly $200 billion.[12] In fact, the data marketplace is so sophisticated that consumers can actually sell their personal identifying information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[13] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[14] Users of the personal data collection app Streamlytics can earn up

---

[11] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

[12] *See* https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Feb. 1, 2024).

[13] *See* https://www.standardbank.co.za/southafrica/personal/products-and-services/security-centre/bank-safely/bank-securely-with-a-digital-id (last visited Feb. 1, 2024).

[14] *See* Nielsen Computer & Mobile Panel, *Frequently Asked Questions,* available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Feb. 1. 2024).

to $200 a month by selling their personal information to marketing companies who use it to build consumer demographics profiles.[15]

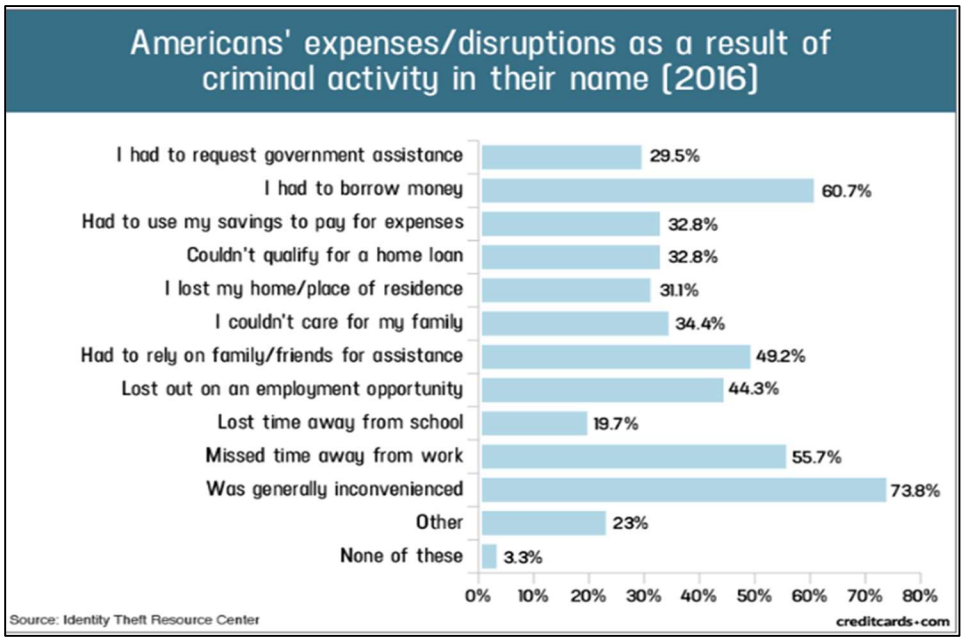
65. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not by a price at which consumers themselves actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it. For example, Plaintiff and Class Members were only to obtain services from Defendant after providing it with their PII. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit or offered credit at unreasonable rates. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

66. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

67. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs their ability to participate in the economic marketplace.

[15] *See* How To Sell Your Own Data And Why You May Want to, available at https://www.mic.com/impact/selling-personal-data-streamlytics (last accessed Feb. 1, 2024).

68. A study by the Identity Theft Resource Center[16] shows the multitude of harms caused by fraudulent use of PII:



69. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[17]

> [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 the Web, fraudulent use of that information may continue for years. As a result,

---

[16] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited June 5, 2024).

[17] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited June 5, 2024).

> studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

70. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

71. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

F. Plaintiff's and Class Members' Damages

Plaintiff Christina Xian's Experience

72. Plaintiff Xian was a customer of Defendants leading up to the date of the Data Breach. When Plaintiff Xian first utilized Defendants' services, Defendants required that she provide them with substantial amounts of her PII.

73. On or about May 21, 2024, Plaintiff Xian received a notice through her PayPal account, which was linked with her account with Defendants in order to make payments, alerting her that someone had purchased 4 resale tickets – totaling $2,500 – on her Ticketmaster account.

74. Thus, Plaintiff Xian suffered actual injury in the form of fraudulent charges to her Ticketmaster account, as well as the time spent dealing with the Data Breach as a result. Plaintiff Xian now also suffers from the present and continuing risk of fraud resulting from the Data Breach, as well as the time she now must spend monitoring her accounts for additional fraud.

75. Plaintiff Xian would not have provided her PII to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their customers' personal information from theft, and that those systems were subject to a data breach.

76. Plaintiff Xian suffered actual injury in the form of having her PII compromised and/or stolen as a result of the Data Breach.

77. Plaintiff Xian further suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that Plaintiff Xian entrusted to Defendants for the purpose of receiving ticketing services from Defendants and which was compromised in, and as a result of, the Data Breach.

78. Plaintiff Xian suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her PII being placed in the hands of criminals.

79. Plaintiff Xian has a continuing interest in ensuring that her PII, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

80. As a result of the Data Breach, Plaintiff Xian made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, as well as long-term credit monitoring options she will now need to use. Plaintiff Xian has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

81. As a result of the Data Breach, Plaintiff Xian has suffered anxiety as a result of the release of her PII to cybercriminals, which PII she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of committing cyber and other crimes against her. Plaintiff Xian is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

82. Plaintiff Xian also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII, a form of property that Defendants obtained from Plaintiff Xian; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

83. As a result of the Data Breach, Plaintiff Xian anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

84. In sum, Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

85. Plaintiff and Class Members entrusted their PII to Defendants in order to receive Defendants' services.

86. Plaintiff's PII was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendants' inadequate data security practices.

87. As a direct and proximate result of Defendants' actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, credit card fraud, phone or utilities fraud, bank fraud, and other forms of identity theft.

88. Further, as a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

89. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their PII, since potential fraudsters will likely use such PII to carry out such targeted schemes against Plaintiff and Class Members.

90. The PII maintained by and stolen from Defendants' systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

91. Plaintiff and Class Members also lost the benefit of the bargain they made with Defendants. Plaintiff and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiff and Class Members paid to Defendants was intended to be used by Defendants to fund adequate security of Defendants' system and protect Plaintiff's and Class Members' PII. Thus, Plaintiff and the Class did not receive what they paid for.

92. Additionally, as a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

93. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

94. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. The contractual bargain entered into between Plaintiff and Defendants included Defendants' contractual obligation to provide adequate data security, which Defendants failed to provide. Thus, Plaintiff and Class Members did not get what they bargained for.

95. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;
b. Canceling and reissuing credit and debit cards;
c. Addressing their inability to withdraw funds linked to compromised accounts;
d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
f. Contacting financial institutions and closing or modifying financial accounts;
g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
h. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and
i. Closely reviewing and monitoring bank accounts for additional unauthorized activity for years to come.

96. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to still be in the possession of Defendants, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not

accessible online, that access to such data is password-protected, and that such data is properly encrypted.

97. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

98. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

99. Specifically, Plaintiff proposes the following Nationwide Class, as well as the following State Subclass definition (also collectively referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had PII stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.
>
> **California Subclass**
>
> All residents of California who had PII stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

100. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which it has a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

101. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class, as well as the California Subclass before the Court determines whether certification is appropriate.

102. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

103. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of hundreds of millions of customers of Defendants whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendants' records, Class Members' records, publication notice, self-identification, and other means.

104. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;
b. Whether Defendants' conduct violated the CCPA invoked below;
c. When Defendants learned of the Data Breach;
d. Whether Defendants' response to the Data Breach was adequate;
e. Whether Defendants unlawfully lost or disclosed Plaintiff's and Class Members' PII;
f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

g. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendants owed a duty to Class Members to safeguard their PII;

j. Whether Defendants breached their duty to Class Members to safeguard their PII;

k. Whether hackers obtained Class Members' PII via the Data Breach;

l. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

n. What damages Plaintiff and Class Members suffered as a result of Defendants' misconduct;

o. Whether Defendants' conduct was negligent;

p. Whether Defendants' conduct was *per se* negligent;

q. Whether Defendants were unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

105. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

106. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

107. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

108. Superiority. A class action is superior to other available methods 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. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action

as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

109. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

110. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

111. Plaintiff restates and realleges all of the allegations stated above and hereafter as if fully set forth herein.

112. Defendants knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

113. Defendants knew or should have known of the risks inherent in collecting the PII of Plaintiff and Class Members and the importance of adequate security. Defendants were on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

114. Defendants owed a duty of care to Plaintiff and Class Members whose PII was entrusted to them. Defendants' duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting PII in their possession;

b. To protect customers' PII using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of PII in their possession;

d. To employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to the FTCA and California consumer protection laws;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

115. Defendants' duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

116. Defendants' duty also arose because Defendants were bound by industry standards to protect their customers' confidential PII.

117. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants, and Defendants owed them a duty of care to not subject them to an unreasonable risk of harm.

118. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within Defendants' possession.

119. Defendants, by their actions and/or omissions, breached their duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members.

120. Defendants, by their actions and/or omissions, breached their duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose PII was compromised.

121. Pursuant to Section 5 of the FTCA, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiff and Class Members.

122. Defendants breached their duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

123. Plaintiff and Class Members are within the class of persons that the FTCA is intended to protect.

124. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the PII compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Defendants' duty in this regard.

125. Defendants violated the FTCA by failing to use reasonable measures to protect the PII of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

126. It was reasonably foreseeable, particularly given the growing number of data breaches of PII, that the failure to reasonably protect and secure Plaintiff's

and Class Members' PII in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendants' networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted PII.

127. Defendants' violations of the FTCA constitute negligence *per se*.

128. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to periodically ensure that their email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to comply with the FTCA;

129. Defendants had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Defendants with their PII was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems (and the PII that it stored on them) from attack.

130. Defendants' breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised, exfiltrated, and misused, as alleged herein.

131. Defendants' breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their PII, and/or loss of time and money to monitor their accounts for fraud.

132. As a result of Defendants' negligence in breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

133. Defendants also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the Data Breach.

134. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

135. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

136. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

137. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

138. Plaintiff restates and realleges the allegations in all preceding paragraphs as if fully set forth herein.

139. Defendants provide ticketing and event services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendants

regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for tickets and events from Defendants.

140. Through Defendants' sale of tickets and events, they knew or should have known that they must protect Plaintiff's and Class Members' confidential PII in accordance with Defendants' policies, practices, and applicable law.

141. As consideration, Plaintiff and Class Members paid money to Defendants and turned over valuable PII to Defendants. Accordingly, Plaintiff and Class Members bargained with Defendants to securely maintain and store their PII.

142. Defendants accepted possession of Plaintiff's and Class Members' PII for the purpose of providing ticket and event services to Plaintiff and Class Members.

143. In delivering their PII to Defendants and paying for tickets and event services, Plaintiff and Class Members intended and understood that Defendants would adequately safeguard the PII as part of that service.

144. Defendants' implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to PII also protect the confidentiality of that data; (2) taking steps to ensure that the PII that is placed in the control of their employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the PII against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

145. Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of such an implied contract.

146. Had Defendants disclosed to Plaintiff and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and Class Members would not have provided their PII to Defendants.

147. Defendants recognized that Plaintiff's and Class Member's PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

148. Defendants violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' PII.

149. Plaintiff and Class Members have been damaged by Defendants' conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class)

150. Plaintiff restates and realleges the allegations in all preceding paragraphs as if fully set forth herein.

151. This Count is pleaded in the alternative to Counts III above.

152. Plaintiff and Class Members conferred a benefit on Defendants by turning over their PII to Defendants and by paying for tickets and event services that should have included cybersecurity protection to protect their PII. Plaintiff and Class Members did not receive such protection.

153. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including from payments made to it by Plaintiff and Class Members.

154. As such, a portion of the payments made by Plaintiff and Class Members is to be used to provide a reasonable and adequate level of data security

that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

155. Defendants have retained the benefits of their unlawful conduct, including the amounts of payment received from Plaintiff and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

156. Defendants knew that Plaintiff and Class Members conferred a benefit upon them, which Defendants accepted. Defendants profited from these transactions and used the PII of Plaintiff and Class Members for business purposes, while failing to use the payments they received for adequate data security measures that would have secured Plaintiff's and Class Members' PII and prevented the Data Breach.

157. If Plaintiff and Class Members had known that Defendants had not adequately secured their PII, they would not have agreed to provide such PII to Defendants.

158. Due to Defendants' conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendants to be permitted to retain the benefit of their wrongful conduct.

159. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remains in Defendants' possession

and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

160. Plaintiff and Class Members are entitled to full refunds, 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. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

161. Plaintiff and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV

VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT OF 2018 CAL. CIV. CODE § 1798.100 ET SEQ. ("CCPA")

(On behalf of Plaintiff and the California Subclass)

162. Plaintiff restates and realleges the allegations in all preceding paragraphs as if fully set forth herein.

163. In 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

164. As fully alleged above, Defendants are subject to the CCPA and failed to implement these procedures or otherwise comply with the CCPA, which resulted in the Data Breach.

165. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure because of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

166. Plaintiff is a "consumer" as defined by Civ. Code § 1798.140(g) because she is natural person residing in the state of California.

167. Defendants are "business[es]" as defined by Civ. Code, § 1798.140(c).

168. The CCPA provides that "personal information" includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted . . . (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." *See* Civ. Code, § 1798.150(a)(1); Civ. Code, § 1798.81.5(d)(1)(A).

169. The information of Plaintiff's and the California Subclass that was compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA.

170. The Data Breach occurred because of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and as a result, Plaintiff's private information was unlawfully accessed.

171. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

172. Simultaneously herewith, Plaintiff provided notice to Defendants, pursuant to Civ. Code, § 1798.150(b)(1), identifying the specific provisions of the CCPA Plaintiff alleges Defendants have violated or are violating. If Defendants have not cured or are unable to cure the violations described therein within thirty days of receipt, Plaintiff will amend her complaint to seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. See Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

173. On behalf of herself and other members of the California Subclass, Plaintiff seeks actual damages, injunctive relief, including public injunctive relief and declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT V

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW CAL. BUS. CODE § 17200, ET SEQ. ("UCL")

(On behalf of Plaintiff and the California Subclass)

174. Plaintiff restates and realleges the allegations in all preceding paragraphs as if fully set forth herein.

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

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

177. Defendants' unlawful, unfair acts and deceptive acts and practices include:

a. Defendants failed to implement and maintain reasonable security measures to protect Plaintiff and the Class Members from unauthorized

disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Defendants failed to:

i. Secure their e-commerce website;

ii. Secure access to their servers;

iii. Comply with industry standard security practices;

iv. Employ adequate network segmentation;

v. Implement adequate system and event monitoring;

vi. Utilize modern payment systems that provided more security against intrusion;

vii. Install updates and patches in a timely manner, and

viii. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

c. Defendants failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the Class Members whose PII has been compromised;

d. Defendants' failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumer data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTCA, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code § 1798.81.5 *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*;

e. Defendants' failure to implement and maintain reasonable security measures also lead to substantial injuries, as described above, that are

not outweighed by any countervailing benefits to consumers or competition. Moreover, because Plaintiff and the Class Members could not know of Defendants' inadequate security, consumers could not have reasonably avoided the harms that Defendants caused;

f. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and the Class Members' PII, including by implementing and maintaining reasonable security measures;

g. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Class Members' PII, including duties imposed by the FTCA, 15 U.S.C § 45; California's Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.*; and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and the Class Members' PII;

i. 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's and the Class Members' PII, including duties imposed by the FTCA, 15 U.S.C § 45; California's Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.*; and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*; and

j. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

178. Defendants' representations and omissions to Plaintiff and the Class Members were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the privacy of consumers' PII.

179. Had Defendants timely disclosed to Plaintiff and the Class Members that their 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 received, maintained, and compiled Plaintiff's and the Class Members' PII as part of the ticketing and event services Defendants provided without advising Plaintiff and the Class Members that Defendants' data security practices were insufficient. Accordingly, Plaintiff and the Class Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

180. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and the Class Members' rights.

181. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff and the Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages as described herein and as will be proved at trial.

182. Plaintiff and the Class 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 PII; declaratory relief; injunctive relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; and other appropriate equitable relief.

183. Plaintiff and the Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all Class Members.

COUNT VI

VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT CAL. CIV. CODE § 1750 ET SEQ. ("CLRA")

(On behalf of Plaintiff and the California Subclass)

184. Plaintiff restates and realleges the allegations in all preceding paragraphs as if fully set forth herein.

185. 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.

186. Defendants are "person[s]" as defined by Civil Code §§ 1761(c) and 1770 and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

187. Plaintiff Xian 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.

188. 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 by:

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.

189. 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.

190. Had Defendants disclosed to Plaintiff and California Subclass Members that their data systems were not secure and, thus, were 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. Defendants were trusted with sensitive and valuable PII regarding hundreds of millions of consumers, including Plaintiff and California Subclass Members. Defendants accepted the responsibility of protecting the data but kept the inadequate state of their security controls secret from the public. Accordingly, Plaintiff and California Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

191. 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, as described herein, including but not limited to 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; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

192. Plaintiff and the California Subclass seek injunctive relief, including an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA. Pursuant to Cal. Civ. Code § 1782(a), Plaintiff served Defendants with notice of their alleged violations of the CLRA by certified mail return receipt requested. If, within thirty days after the date of such notification, Defendants fail to

provide appropriate relief for their violations of the CLRA, Plaintiff will amend this Complaint to seek damages.

COUNT VII
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT, CIV. CODE § 1798.80, ET SEQ. ("CCRA")

193. Plaintiff incorporates and realleges the foregoing allegations of fact.

194. Plaintiff and Class Members are "customers" within the meaning of Civil Code section 1798.80(c), as they provided personal information to DRSI for the purpose of obtaining services.

195. Defendants are a "business" within the meaning of Civil Code section 1978.80(a).

196. The CCRA provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California . . . whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person . . . in the most expedient time possible and without unreasonable delay[.]" Civ. Code § 1798.82.

197. The Data Breach was a breach of security within the meaning of section 1798.82. PII stolen in the Data Breach, such as names, addresses, phone numbers, and payment card details, constitutes "personal information" within the meaning of section 1798.80(e).

198. As a result of Defendants' delay in notifying Plaintiff and Class Members of the Data Breach, Plaintiff and Class Members were deprived of an opportunity to take timely and appropriate self-protective measures, such as requesting a credit freeze. In addition, as a result of the delay, Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other

injuries and actual harm including, without limitation: (1) the compromise and theft of their personal information; (2) loss of the opportunity to control how their personal information is used; (3) diminution in the value and use of their personal information entrusted to Defendant with the understanding that Defendant would safeguard it against theft and not allow it to be accessed and misused by third parties; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identity theft and misuse of their personal information; (5) continued undue risk to their personal information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

199. Therefore, on behalf of the Class, Plaintiff seeks actual damages under Civil Code section 1798.84(b), injunctive and declaratory relief, and any other relief deemed appropriate by the Court.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Classes described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class and California Subclass requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: June 5, 2024

Respectfully submitted,

/s/ John J. Nelson
John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive, Penthouse
Beverly Hills, CA 90212
Tel: (858) 209-6941
jnelson@milberg.com

Mason A. Barney *
Tyler J. Bean *
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com

E: tbean@sirillp.com

Counsel for Plaintiff and the Proposed Class

* Application for *Pro Hac Vice* Admission Forthcoming