STEVEN A. SCHWARTZ*
steveschwartz@chimicles.com
BEENA M. MCDONALD*
bmm@chimicles.com
ALEX M. KASHURBA*
amk@chimicles.com
MARISSA N. PEMBROKE*
mnp@chimicles.com
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500

JAMES J. ROSEMERGY*
jrosemergy@careydanis.com
CAREY, DANIS & LOWE
8235 Forsyth, Suite 1100
St. Louis, MO 63105
Telephone: (314) 725-7700

DAVID B. JONELIS (BAR NO. 265235)
djonelis@lavelysinger.com
LAVELY & SINGER PC
2049 Century Park East, Suite 2400
Los Angeles, California 90067-2906
Telephone: (310) 556-3501

Attorneys for Plaintiffs and
the Proposed Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

JODI CABALLERO, OWEN CONLAN, BRYAN CURTIS, KELLEY DAVIS, CHARLES FITZGERALD, BRENDAN HEALY, CHRIS RIPPEL, and MICHAEL WALTERS, individually and on behalf of all others similarly situated, Plaintiffs, vs. LIVE NATION ENTERTAINMENT, INC., and TICKETMASTER, LLC, Defendants.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs JODI CABALLERO, OWEN CONLAN, BRYAN CURTIS, KELLEY DAVIS, CHARLES FITZGERALD, BRENDAN HEALY, CHRIS RIPPEL, and MICHAEL WALTERS ("Plaintiffs"), individually and on behalf of others similarly situated, bring this class action complaint against Defendants, LIVE NATION ENTERTAINMENT, INC., and TICKETMASTER, LLC ("Live Nation" and "Ticketmaster", or collectively, "Defendants"). Plaintiffs allege as follows upon personal knowledge as to their own acts and experiences, and upon the investigation of their attorneys as to all other matters.

INTRODUCTION

1. This is a data breach class action on behalf of consumers whose Personally Identifying Information ("PII") was stolen by cybercriminals as part of a major cyber-attack on Defendants' systems. On or about May 20, 2024, Live Nation detected suspicious activity within Defendants' network containing data from Ticketmaster and thereafter concluded that there was unauthorized access to Plaintiffs' and many other individuals' PII (the "Data Breach").[1] PII compromised in the breach includes full names, email address, phone numbers, order history, including prior tickets purchased, payment information, including partial credit card numbers, expiration dates, and other sensitive and private data.

2. One week later, on May 27, 2024, the notorious hacker group known as ShinyHunters took responsibility for the Data Breach – gaining access to 1.3 terabytes of PII of roughly 560,000,000 individuals – and offered the stolen data for sale on the dark web from BreachForums, an infamous hacking forum and marketplace for cybercriminals to buy and sell stolen data.[2]

[1] United States Securities and Exchange Commission, Live Nation Entertainment, Inc., Form 8-K, available at: https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm.

[2] Waqas, *Hackers Claim Ticketmaster Data Breach: 560M Users' Info for Sale at $500k*, HACKREAD (May 29, 2024), https://hackread.com/hackers-ticketmaster-data-breach560m-users-sale/ (last visited June 2, 2024).

3. Ticketmaster is an American subsidiary of the global entertainment conglomerate, Live Nation. Ticketmaster is the global leader for ticket management and ticket sales for a wide array of events such as concerts, sports, art, theater, and family activities.[3] Ticketmaster specializes in the sales, marketing, and distribution of tickets.[4]

4. As a condition of purchasing tickets, Defendants' customers are required to provide and entrust Defendants with sensitive and private information, including PII. By taking possession and control of their information, Defendants assumed a duty to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect individuals PII from unauthorized disclosure.

5. The exposure of a person's PII through a data breach substantially increases that person's risk of identity theft, fraud, and similar forms of criminal mischief, potentially for the rest of their lives. Mitigation of such risk requires individuals to expend a significant amount of time and money to closely monitor their credit, financial accounts and email accounts. Mitigation of the risk of misuse of their sensitive and private information may not even be possible.

6. As of the date of this filing, Defendants have offered no assurance that the sensitive and private information that was accessed in the Data Breach has been recovered or destroyed.

7. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiffs' and Class Members' PII was accessed and disclosed. Plaintiffs and Class Members are now at a substantially increased risk of experiencing misuse of their PII in the coming years. Additionally, Plaintiffs and Class Members have a current and now-existing injury in that their PII is in the hands of those with ill intent, requiring current action on their part to lessen the likelihood of future negative repercussions. This action seeks to remedy these failings and their consequences.

---

[3] *See* https://www.ticketmaster.com/.
[4] *See* https://www.livenation.com/ticketmaster/.

8. This injury to Plaintiffs and Class Members is compounded by the fact that Defendants failed to timely notify the public of the Data Breach. Defendants' failure to timely notify the victims of the Data Breach meant that Plaintiffs and Class Members were unable to take timely and proactive measures to prevent or mitigate the resulting harm.

9. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was stolen in the Data Breach. Plaintiffs assert claims for negligence, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations of California's consumer protection statutes, and seek declaratory relief, injunctive relief, monetary damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiffs

10. Plaintiff Jodi Caballero is a resident of Lake May, Florida and has had a Ticketmaster account since at least 2010. Plaintiff has a current and active Ticketmaster account as of the date of filing.

11. Plaintiff Owen Conlan is a resident of Delaware, Ohio and has had a Ticketmaster account since at least 2011. Plaintiff has a current and active Ticketmaster account as of the date of filing.

12. Plaintiff Bryan Curtis is a resident of Ontario, New York and has had a Ticketmaster account since at least 2012. Plaintiff has a current and active Ticketmaster account as of the date of filing.

13. Plaintiff Kelley Davis is a resident of Saint Louis, Missouri and has had a Ticketmaster account since at least 2013. Plaintiff has a current and active Ticketmaster account as of the date of filing.

14. Plaintiff Charles Fitzgerald is a resident of Buffalo, New York and has had a Ticketmaster account since at least 2013. Plaintiff has a current and active Ticketmaster account as of the date of filing.

15. Plaintiff Brendan Healy is a resident of Austin, Texas and has had a Ticketmaster account since at least 2019. Plaintiff has a current and active Ticketmaster account as of the date of filing.

16. Plaintiff Chris Rippel is a resident of Elk Grove, California and has had a Ticketmaster account since at least 2013. Plaintiff has a current and active Ticketmaster account as of the date of filing.

17. Plaintiff Michael Walters is a resident of Oak Park, Illinois and has had a Ticketmaster account since at least 2008. Plaintiff has a current and active Ticketmaster account as of the date of filing.

Defendant Live Nation Entertainment, Inc.

18. Defendant Live Nation Entertainment, Inc. is a Delaware corporation with its principal place of business located at 9348 Civic Center Drive, Beverly Hills, CA 90210. Live Nation also maintains offices all over the globe.

Defendant Ticketmaster, LLC.

19. Defendant Ticketmaster, LLC, is a wholly owned subsidiary of Live Nation Entertainment, Inc. It shares its principal place of business with Live Nation located at 9348 Civic Center Drive, Beverly Hills, CA 90210.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million dollars, exclusive of interest and costs, and is a class action in which some members of the class are citizens of states different than Defendants. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

21. This court has personal jurisdiction over Defendants because Defendants are headquartered in this District, regularly conduct business in this state, and the acts and omissions giving rise to Plaintiffs' claims emanated from within this District.

22. Venue is proper under 18 U.S.C. § 1391(b) because Defendants' headquarters are in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Defendants Collect and Store PII

23. Defendant Live Nation Entertainment, Inc., is an American multinational entertainment company which promotes, operates, and manages major live events.[5]

24. Defendant Ticketmaster, LLC is a wholly owned subsidiary of Defendant Live Nation and is the premier booking and ticketing service provider for the arts and entertainment industries. It is responsible for ticketing major events within these industries across the globe. Ticketing services generally occur online or through mobile apps but can occur over the phone.[6]

25. In 2010, after years of competition, Defendants merged to combine forces and thereafter began buying out other competitors and offering incentives to artists and venues to use their services.[7]

26. Defendant Ticketmaster presently controls about 70% of the market for ticketing services.[8] Individuals looking to buy and sell tickets for most major events are thus forced to use Defendants' services, and in some markets, consumers literally have no other options for ticketing. Thus, consumers wanting to attend events have no alternative

---

[5] *See* https://www.livenation.com/.

[6] *See* Ticketmaster, LLC's Form 10-K filed with the United States Securities and Exchange Commission, available at: https://investors.livenationentertainment.com/sec-filings/annual-reports/content/0001335258-22-000019/0001335258-22-000019.pdf (last visited May 31, 2024).

[7] Adam Hayes, *Is Ticketmaster a Monopoly?*, Investopedia, February 18, 2023, available at https://www.investopedia.com/is-ticketmaster-a-monopoly-6834539.

[8] Mae Anderson, *The DOJ is suing Ticketmaster and Live Nation. What does that mean for concertgoers?*, ABC 12 News, May 28, 2024, available at: https://www.12newsnow.com/article/news/entertainment-news/the-justice-department-is-suing-ticketmaster-and-live-nation-what-does-that-mean-for-concertgoers-music/507-868733d3-5f28-4888-8f5f-0dc6af0cc6b2#:~:text=promoter%20Live%20Nation.-,Attorney%20General%20Merrick%20Garland%20said%20the%20aim%20is%20to%20allow,controls%20a%20whopping%2070%25%20of.

that does not require disclosure of their PII to Defendants.

27. The monopoly formed by Defendants has drawn the attention of the Department of Justice, which recently filed a civil antitrust suit against Defendants in the United States District Court for the Southern District of New York for monopolization and other unlawful conduct that "thwarts competition in markets across the entertainment industry."[9]

28. Defendants' allegedly anticompetitive conduct has certainly paid off. Before the COVID-19 pandemic, Defendant Ticketmaster was selling nearly half a billion tickets worldwide.[10] Its concert business alone generated $4.7 billion for the company in 2021.[11]

29. To purchase tickets for sale from Ticketmaster, an individual is required to provide PII such as their name, contact information and payment information.

30. As a condition of providing these services to its customers, Ticketmaster requires that they "first create a Ticketmaster account and provide personal information."[12] Thus, Ticketmaster requires its customers entrust it with sensitive and private information such as PII. Defendants collect and maintain such information on their servers.

31. Due to the highly sensitive nature of the information Defendants collect and maintain, Defendants promised to provide confidentiality and adequate security for their customers' data through their applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

32. Indeed, Defendant Ticketmaster's Privacy Policy on its website promises: "You can trust us with your personal information, so we strive to always be clear and

---

[9] Department of Justice, Press Releases, *Justice Department Sues Live Nation-Ticketmaster for Monopolizing Markets Across Live Concert Industry*, May 23, 2024, available at: https://www.justice.gov/opa/pr/justice-department-sues-live-nation-ticketmaster-monopolizing-markets-across-live-concert.

[10] *Supra* n.6.

[11] *Id.*

[12] Ticketmaster, Privacy Policy, available at: https://privacy.ticketmaster.com/privacy-policy.

honest about how and why we will use it."[13]

33. Further, Ticketmaster states that it employs security measures to protect individuals' information, which includes:

- Deletion of account data at the request of the user within a maximum of 90 days of the request;
- Deletion of account data after 7 years of inactivity within the account; and
- Maintaining limited information in separate databases to keep its platform safe and secure from fraud and cyber-attacks.[14]

34. On information and belief, the type of information that Defendants maintain includes, *inter alia*: full name, email address, physical address, date of birth, credit/debit card information, order history photo identification, and any other information necessary to provide their services. Ticketmaster also collects the IP addresses of customers using its services on its website or apps.[15]

35. In the course of their relationship, Plaintiffs and Class Members provided Defendants with at least their PII.

36. Plaintiffs and Class Members, as current customers of Defendants, relied on Defendant Ticketmaster's promise to keep their sensitive PII confidential and secured, to use such information for business purposes only, and to make only authorized disclosures of this information.

Defendants Knew that Criminals Target Valuable PII and Failed to Take Action to Prevent Theft

37. At all relevant times, Defendants knew they were storing sensitive PII and that, as a result, Defendants' systems would be attractive targets for cybercriminals.

---

[13] *Id.*

[14] Ticketmaster, Looking After Your Information, available at: https://privacy.ticketmaster.com/privacy-policy#looking-after-your-information.

[15] *Supra* n.12.

38. Defendants also knew that a breach of their systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against all individuals whose PII was compromised.

39. The risks are not theoretical. The prevalence of data breaches has increased dramatically over the years: "The number of reported data breaches in the U.S. rose to a record 3,205 in 2023, up 78% from 2022 and 72% from the previous high-water mark in 2021, according to the nonprofit Identity Theft Resource Center."[16]

40. In recent years, numerous high-profile breaches have occurred including breaches involving MoveIt, First American Financial Corp., JP Morgan Chase & Co., and Equifax.

41. In tandem with the increase in data breaches, the rate of identity theft has increased. Since 2019, identity theft reports have increased $68.3%. In the second quarter of 2023, roughly 277,620 ID theft reports were submitted to the Federal Tarde Commission, which was a substantial increase from the 164,982 reported in the same quarter in 2019.[17]

42. Every state has experienced an increase in identity theft over 11% per 100,000 residents since 2019.[18]

43. PII has considerable value to hackers. Hackers sell stolen data on the black market through the "proliferation of open and anonymous cybercrime forums on the Dark Web that server as a bustling marketplace for such commerce."[19]

---

[16] Stuart Madnick, *If Companies Are So Focused on Cybersecurity, Why Are Data Breaches Still Rising?*, THE WALL STREET JOURNAL (Mar. 15, 2024), https://www.wsj.com/tech/cybersecurity/why-are-cybersecurity-data-breaches-still-rising-2f08866c (last visited May 17, 2024).

[17] Julie Ryan Evans, *93 of 100 Largest US Metros and All States Hae Seen Increase in ID Theft Reports Since 2019*, LENDINGTREE (Nov. 6, 2023), https://www.lendingtree.com/insurance/id-theft-study/#:~:text=Identity%20theft%20reports%20have%20increased,the%20same%20quarter%20in%202019 (last visited May 17, 2024).

[18] *Id.*

[19] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited May 17, 2024).

8*Data Breach Report: 2021 Year End*, Risk Based Security (February 4, 2022),

44. The breadth of data that can be bought and sold leaves Defendants' customers especially vulnerable to identity theft, tax fraud, credit and bank fraud.

45. Even basic or partial information in the hands of bad actors can be used in phishing scams to steal more information from individuals. A phishing email will be tailored to the information known about the individual to appear more legitimate, and thus the individual is more likely to provide additional sensitive information. For example, a bad actor with an individual's email address and name can formulate an email stating the individuals' passwords and providing a link for the individual to hand over the key to their accounts.

46. Lately, the number of phishing schemes is on the rise and the schemes themselves are becoming more sophisticated. In 2023, the number of phishing attacks increased by 58.2%.[20] Experts expect this trend to continue with the introduction of artificial intelligence.[21]

47. Due to the prevalence of identity theft, consumers place a high value on the privacy of their data. Studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[22]

48. Recently, more consumers are exercising their Data Subject Access Rights and leaving providers over their data practices and policies.[23]

---

https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/ (last visited Apr. 26, 2024).

[20] "Phishing Attacks Rise 58% in the Year of AI: ThreatLabz 2024 Phishing Report, April 23, 2024, available at https://www.zscaler.com/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report.

[21] *See, e.g.*, "AI Will Increase the Quantity – and Quality – of Phishing Scams", Harvard Business Review, May 30, 2024, available at https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams.

[22] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), available for download at: https://www.jstor.org/stable/23015560?seq=1.

[23] CISCO, *Cisco 2023 Consumer Privacy Survey* (April 2023), available at https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html?CCID=cc000742

49. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

50. Defendants certainly knew and understood that unprotected or exposed PII in their custody is highly valuable and sought after by nefarious criminals seeking to illegally monetize that PII through unauthorized access.

51. Armed with this knowledge, Defendants breached their duties by failing to implement and maintain reasonable security measures to protect Plaintiffs' and Class members' PII from being stolen.

The Data Breach

52. On or about May 20, 2024, Defendants detected suspicious activity within their systems.[24] In response, they, along with industry leading forensic investigators, initiated an investigation into the incident to determine whether customer data was leaked as a result.[25]

53. Shortly thereafter, it was reported that the ransomware group ShinyHunters had taken responsibility for the Data Breach and had stolen 1.3 terabytes of customer data from Defendants' systems containing data from Ticketmaster which comprised the sensitive information and PII of roughly 560 million individuals, including Plaintiffs and Class Members.[26]

54. On May 27, 2024, ShinyHunters offered the stolen data for sale on the dark web, on a notorious data breach forum known as BreachForums for $500,000.[27]

55. Defendants have yet to publicly acknowledge the Data Breach. However, on May 31, 2024, Live Nation filed a brief Form 8-K with the United States Securities and Exchange Commission and made the following statement about the Data Breach:

---

[24] *Supra* n.1.
[25] *Id.*
[26] *Supra* n. 2.
[27] *Id.*

> "On May 20, 2024, Live Nation Entertainment, Inc. (the "Company" or "we") identified unauthorized activity within a third-party cloud database environment containing Company data (primarily from its Ticketmaster L.L.C. subsidiary) and launched an investigation with industry-leading forensic investigators to understand what happened. On May 27, 2024, a criminal threat actor offered what it alleged to be Company user data for sale via the dark web. We are working to mitigate risk to our users and the Company, and have notified and are cooperating with law enforcement. As appropriate, we are also notifying regulatory authorities and users with respect to unauthorized access to personal information.
>
> As of the date of this filing, the incident has not had, and we do not believe it is reasonably likely to have, a material impact on our overall business operations or on our financial condition or results of operations. We continue to evaluate the risks and our remediation efforts are ongoing."[28]

56. Upon information and belief, the cyberattack was targeted at Defendants, due to their status as a monopolistic enterprise that collects, creates, and maintains PII on computer networks and/or systems.

57. Plaintiffs' and Class Members' PII was compromised and acquired in the Data Breach.

58. Due to this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendants that included the PII of Plaintiffs and Class Members.

59. As evidenced by the Data Breach's occurrence, the PII contained on Defendants' systems was not encrypted. Had it been, the data thieves would have stolen only unintelligible data.

60. Moreover, the security measures as indicated by Defendant Ticketmaster on its website were clearly ineffective at deterring the attack and keeping Plaintiffs' and

[28] *Supra* n.1.

Class Members' PII safe and secure.

61. Plaintiffs now believe that their PII was or will soon be purchased from the dark web, and used in fraudulent crimes, as that is the *modus operandi* of cybercriminals.

Plaintiffs' Experiences are Demonstrative of the Problem

62. Plaintiffs each purchased tickets using Defendants' platforms for various events.

63. In connection with these transactions, Defendants required Plaintiffs to provide their PII, including full name, mailing address, and credit card or other financial account information when purchasing these tickets. Sellers of tickets on Defendants' platforms were also required to provide social security numbers, upon information and belief.

64. Upon information and belief, Defendants retained Plaintiffs' private information in their systems at the time of the Data Breach.

65. Plaintiffs have not received a breach notification letter in the mail or otherwise from Defendants.

66. Plaintiffs are conscientious with their private information. Plaintiffs do not knowingly transmit unencrypted private information over the internet or any other unsecured medium. Plaintiffs would not have entrusted their private information with Ticketmaster had they known of Defendants' failure to implement and maintain data security measures.

67. Plaintiffs' PII was exposed and accessed in the Data Breach.

68. As a result, Plaintiffs have had to spend time and resources monitoring their credit reports and financial accounts for fraudulent activity, setting up fraud alerts for impacted credit accounts, and otherwise taking steps to mitigate the risk posed by the release of their PII to hackers.

69. Indeed, at least one Plaintiff – Michael Walters – has already seen concerning activity associated with a credit card he used with his Ticketmaster account. On or about June 2, 2024, he became aware of five unauthorized charges on a credit card

linked to his Ticketmaster account. Those charges are currently being disputed and under investigation.

70. Plaintiffs are now at a substantial risk of identity theft and/or fraud, and will spend future time and resources to monitor their accounts and mitigate their risks, time they would not have to spend but for the Data Breach.

Defendants Failed to Comply with the FTCA and FTC Guidelines

71. The Federal Trade Commission Act ("FTCA") prohibits Defendants from engaging in "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45.

72. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which reflect the importance of implementing reasonable data security practices.

73. The FTC's publication, Protecting Personal Information, established cyber-security guidelines for businesses. The guidelines provide that businesses should take action to protect the personal patient information that they collect; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems.[29]

74. 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 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]

75. The FTC further recommends that businesses not maintain private information longer than is needed for authorization of a transaction; limit access to

[29] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.
[30] *Id.*

sensitive information; require complex passwords be used on networks; use industry-tested methods for security monitor for suspicious activity on the networks; and verify that third-party service providers have implemented reasonable security measures.

76. The FTC has the authority to bring enforcement actions against businesses for failing to protect PII adequately and reasonably under Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

77. The orders that result from enforcement actions further clarify the measures businesses must take to meet their data security obligations.

78. Defendants failed to properly implement basic data security practices.

79. Defendants were at all relevant times fully aware of their obligations to protect their customers' PII, and of the significant consequences that would result from their failure to do so.

80. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to their customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

81. Consequently, cybercriminals circumvented Defendants' lax security measures, resulting in the Data Breach.

Defendants Failed to Comply with Industry Standards

82. Entities like Defendants are particularly vulnerable to cyberattacks because of the sensitive nature of the information that they collect and maintain and the large volume of customers they service..

83. Due to this vulnerability, there are industry best practices that should be implemented by entities like Defendants.

84. These practices include but are not limited to: Educating and training employees about the risks of cyberattacks, strong passwords, multi-layer security such as firewalls, anti-virus and malware software, encryption, multi-factor authentication, backup data, limitation of employees with access to sensitive data, setting up network firewalls, switches and routers, monitoring and limiting the network ports, and

monitoring and limited access to physical security systems.

85. 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.CM8, 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.

86. Defendants' failure to implement the industry standards described herein resulted in the Data Breach and caused injury to Plaintiffs and Class Members.

Common Damages Sustained by Plaintiffs and Class Members

87. For the reasons mentioned above, Plaintiffs and all other Class members have suffered injury and damages directly attributable to Defendants' failure to implement and maintain adequate security measures, including, but not limited to: (i) fraudulent credit card applications attempted in their name (ii) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) invasion of their privacy; (v) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

CLASS ALLEGATIONS

88. Plaintiffs bring this class action individually and on behalf of all persons similarly situated, pursuant to Federal Rule of Civil Procedure 23.

89. Plaintiffs seeks certification of a Nationwide Class, or alternatively the following state subclasses, as defined below and subject to further amendment:

Nationwide Class

All individuals in the United States whose PII was compromised in the Data Breach (the "Class").

California Subclass

All individuals who reside in California and whose PII was compromised in the Data Breach (the "California Subclass").

Florida Subclass

All individuals who reside in Florida and whose PII was compromised in the Data Breach (the "Florida Subclass").

Illinois Subclass

All individuals who reside in Illinois and whose PII was compromised in the Data Breach (the "Illinois Subclass").

Missouri Subclass

All individuals who reside in Missouri and whose PII was compromised in the Data Breach (the "Missouri Subclass").

New York Subclass

All individuals who reside in New York and whose PII was compromised in the Data Breach (the "New York Subclass").

Ohio Subclass

All individuals who reside in Ohio and whose PII was compromised in the Data Breach (the "Ohio Subclass").

Texas Subclass

All individuals who reside in Texas and whose PII was compromised in the Data Breach (the "Texas Subclass").

90. Excluded from the Class are Defendants and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

91. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

92. Numerosity. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. It is reported that approximately 560 million individuals' information was exposed in the Data Breach. The

contact information of those individuals is available from Defendants' business records.

93. Commonality. Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

- Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PII from unauthorized access and disclosure;
- Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII;
- Whether Defendants breached their duties to protect Plaintiffs' and Class members' PII;
- Whether Defendants breached their fiduciary duty to Plaintiffs and Class Members;
- When Defendants learned of the Data Breach;
- Whether Defendants' response to the Data Breach was adequate;
- Whether Defendants knew or should have known that their data security systems and monitoring procedures were deficient;
- Whether hackers obtained Plaintiffs' and Class Members' data in the Data Breach;
- Whether an implied contract existed between Class members and Defendants providing that Defendants would implement and maintain reasonable security measures to protect and secure Class Members' PII from unauthorized access and disclosure;
- Whether Defendants were unjustly enriched;
- Whether Defendants breached their contractual obligations owed to Plaintiffs and the Class;
- Whether Defendants violated the California Unfair Competition Law;
- Whether Defendants violated the California Legal Remedies Act;
- Whether Defendants violated the California Consumer Privacy Act;
- Whether Plaintiffs and Class Members are entitled to injunctive relief and identity theft protection to redress the imminent harm they face due to the Data Breach; and

- Whether Plaintiffs and all other members of the Class are entitled to damages and the measure of such damages and relief.

94. Typicality. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

95. Adequacy of Representation. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or conflict with, the Class they seek to represent. Plaintiffs retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

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

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

98. Finally, class certification is appropriate under Federal Rule of Civil Procedure 23(b). Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

(Plaintiffs, individually and on behalf of the Nationwide Class, or Alternatively, the State Subclasses)

99. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

100. Defendants require that their customers, including Plaintiffs and Class Members, submit private information such as PII in the course of providing their services.

101. Defendants collected, acquired, and stored Plaintiffs' and Class Members' private information on their servers.

102. Plaintiffs and Class Members entrusted Defendants with their private information and had the understanding that Defendants would safeguard their information.

103. Defendants had knowledge of the sensitivity of Plaintiffs' and Class Members' private information, and the consequences that would result from the unauthorized disclosure of such information. Defendants knew that similar entities were the target of cyber-attacks in the past, and that Plaintiffs and Class members were the foreseeable and probable victims in the event of any inadequate data security procedures.

104. It was therefore reasonably foreseeable that the failure to implement adequate data security procedures would result in injuries to the Plaintiffs and Class Members.

105. Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their private information in their possession, custody, or control from the unauthorized disclosure of such information.

106. Defendants' duty to exercise reasonable care arises from several sources, including but not limited to common law, the FTCA, and industry standards.

107. Defendants breached their duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to them—including Plaintiffs' and Class members' PII.

108. As has been widely reported, the PII of Plaintiffs and Class Members was disclosed to unauthorized third persons as a result of the Data Breach.

109. Defendants' negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members caused their PII to be compromised in the Data Breach.

110. Defendants are in exclusive control over their own internal systems (with the exception of malicious hackers who were inexplicably permitted to access them), and Plaintiffs and Class Members were in no position to protect their PII themselves.

111. But for Defendants' breach of the duties described herein, Plaintiffs and Class Members' PII would not have been compromised, and there is a causal relationship between Defendants' failure to implement, control, direct, oversee, manage, monitor, and audit adequate data security procedures to protect the PII of their customers and the harm suffered by Plaintiffs and Class Members.

112. As a direct and proximate result of Defendants' conduct described above, they directly and proximately caused the Data Breach, and Plaintiffs and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are

entitled to compensation; (ii) actual identity theft;(iii) improper disclosure of their PII; (iv) breach of the confidentiality of their PII; (v) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

113. As a direct and proximate result of Defendants' wrongful conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

114. Plaintiffs and Class members are entitled to damages incurred as a result of the Data Breach.

115. Defendants' negligent conduct is ongoing, in that it still holds Plaintiffs' and Class Members PII in an unsafe and insecure manner.

116. Thus, Plaintiffs and Class Members are also entitled to injunctive relief in the form of requiring Defendants to strengthen their data security procedures and to provide credit monitoring to Class Members.

COUNT II

NEGLIGENCE PER SE

(Plaintiffs, individually and on behalf of the Nationwide Class, or alternatively, the State Subclasses)

117. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

118. Defendants' duties arise from, *inter alia*, Section 5 of the FTCA, the UCL, CLRA, and CCPA.

119. Defendants violated Section 5 of the FTCA, the UCL, CLRA and CCPA by failing to implement reasonable measures to protect Plaintiffs' and Class Members' PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the

foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

120. Defendants' violations of Section 5 of the FTCA, the UCL, CLRA and CCPA constitutes negligence *per se*.

121. Plaintiffs and Class members are within the class of persons that Section 5 of the FTCA, the UCLA, CLRA, and CCPA were intended to protect.

122. The harm occurring as a result of the Data Breach is the type of harm that Section 5 of the FTCA, the UCL, CLRA, and CCPA were intended to guard against.

123. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII to unauthorized individuals.

124. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendants' violations of Section 5 of the FTCA, the UCL, CLRA, and CCPA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII/PHI; (iv) breach of the confidentiality of their PII/PHI; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

125. As a direct and proximate result of Defendants' wrongful conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury,

including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

126. Plaintiffs and Class members are entitled to damages incurred as a result of the Data Breach.

127. Plaintiffs and Class Members are also entitled to injunctive relief in the form of requiring Defendants to strengthen their data security procedures and to provide credit monitoring to Class Members.

COUNT III

BREACH OF FIDUCIARY DUTY

(Plaintiffs, individually and on behalf of the Nationwide Class, or alternatively, the State Subclasses)

128. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

129. Plaintiffs and Class members gave Defendants their PII in confidence, believing that Defendants would protect that information. Plaintiffs and Class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiffs' and Class members' PII created a fiduciary relationship between Defendants and Plaintiffs and Class members. In light of this relationship, Defendants must act primarily for the benefit of their customers, which includes safeguarding and protecting Plaintiffs' and Class Members' PII.

130. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. They breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' PII, failing to comply with Section 5 of the FTCA, and otherwise failing to safeguard Plaintiffs' and Class members' PII that they collected.

131. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but

not limited to: (i) a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII; (iv) breach of the confidentiality of their PII; (v) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

COUNT IV

BREACH OF IMPLIED CONTRACT

(Plaintiffs, individually and on behalf of the Nationwide Class, or alternatively, the State Subclasses)

132. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

133. In connection with receiving services from Defendants, Plaintiffs and all other Class members entered into implied contracts with Defendants or were intended third-party beneficiaries of contracts between Defendants and others.

134. Pursuant to these implied contracts, money was paid to Defendants, whether directly from Plaintiffs and Class members or indirectly, and Defendants were provided with the PII of Plaintiffs and Class members. In exchange, Defendants impliedly agreed to, among other things, take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; and protect Plaintiffs' and Class members' PII in compliance with federal and state laws and regulations and industry standards.

135. The protection of PII was a material term of the implied contracts that were either between Plaintiffs and Class members, on the one hand, and Defendants, on the other hand or were between third parties and Defendants, to which Plaintiffs and Class members were intended third party beneficiaries.

136. Plaintiffs and Class members or the third parties fulfilled their obligations under the contracts.

137. Defendants breached their obligations by failing to implement and maintain reasonable data security measures to protect and secure the PII and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

138. Defendants' breach of their obligations of their implied contracts directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

139. Plaintiffs and all other Class members were damaged by Defendants' breach of implied contracts because: (i) they paid—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) they suffered actual identity theft; (iv) their PII was improperly disclosed to unauthorized individuals; (v) the confidentiality of their PII has been breached; (vi) they were deprived of the value of their PII, for which there is a well-established national and international market; and/or (vii) they lost time and money to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

COUNT V

UNJUST ENRICHMENT

(Plaintiffs, individually and on behalf of the Nationwide Class, or alternatively, the State Subclasses)

140. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

141. This count is pleaded in the alternative to Plaintiffs' breach of implied contract claim (Count IV).

142. Plaintiffs and Class members conferred a monetary benefit upon Defendants in the form of monies paid to Defendants and/or their agents for services and/or intangible property.

143. In exchange, Plaintiffs and Class Members should have received from Defendants the services and/or intangible property that were the subject of the transaction and should have had their private information protected with adequate data security procedures.

144. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members by acquiring and/or collecting their private information as well as the payments made on their behalf as a necessary part of obtaining Defendants' services. Defendants appreciated, accepted, and benefitted from the receipt of Plaintiffs' and Class members' private information and payments in that they used the private information and profited from the transactions in furtherance of their business.

145. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class members. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class members is used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

146. Defendants, however, failed to secure Plaintiffs' and Class members' private information and, therefore, did not provide adequate data security in return for the benefit of Plaintiffs and Class members.

147. Defendants would not be able to carry out an essential function of their business without the private information of Plaintiffs and Class members and derived revenue from such information by using it for business purposes. Plaintiffs and Class members expected that Defendants would use a portion of that revenue to fund adequate data security measures.

148. Defendants acquired Plaintiffs' and Class members' private information and

payments through inequitable means in that they failed to disclose the inadequate data security procedures previously alleged herein.

149. If Plaintiffs and Class members knew that Defendants had not reasonably secured their private information, including their PII, they would not have allowed their private information to be provided to Defendants.

150. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' private information. Instead of proving adequate data security measures, Defendants increased their profit at the expense of Plaintiffs and Class members by using cheaper, ineffective security measures.

151. Plaintiffs and Class members on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security and safety of their private information.

152. Plaintiffs and Class members have no adequate remedy at law.

153. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class members because Defendants failed to adequately implement the data privacy and security procedures that Plaintiffs and Class members paid for and that were otherwise mandated by federal and state law, and industry standards.

154. Under principles of equity and good conscience, Defendants should be compelled to provide for the benefit of Plaintiffs and Class members, all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT VI

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL")

Cal. Bus. & Prof. Code §§ 17200–17210

(Plaintiffs, individually and on behalf of the Nationwide Class, or alternatively, the California Subclass)

155. Plaintiffs reallege and incorporate by reference all preceding and succeeding allegations as though fully set forth herein.

156. The UCL broadly proscribes "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

Unlawful Conduct

157. Defendants' conduct is unlawful, and in violation of the UCL, because, as set forth herein, it violates Section 5 of the FTCA, the CLRA and the CCPA through failing to implement adequate safeguards to protect Plaintiffs' and Class members' PII.

Unfair Conduct

158. Defendants' conduct is unfair because it violated California public policy, legislatively declared in the UCL, CLRA, and CCPA.

159. Defendants also acted in an immoral, unethical, oppressive, and unscrupulous manner that is injurious to consumers in that the sensitive personal information of 560 million individuals, including California consumers, has been compromised in the Data Breach and made available on the dark web for criminals to purchase and use for criminal activity, including identity theft and fraud.

160. The gravity of the harm resulting from Defendants' unfair conduct outweighs any potential utility of the conduct, to the extent there is any utility at all. The practice of collecting, storing, and maintaining PII without employing adequate safeguards to protect that information harms the public at large and is part of a common and uniform course of wrongful conduct.

161. There are reasonably available alternatives that would further Defendants' business interests of increasing sales. For example, Defendants could have implemented security measures as laid out for them in guidance from the FTCA, industry standards and the CCPA.

162. The harm from Defendants' unfair conduct was not reasonably avoidable by consumers. Plaintiffs and California Subclass had no reasonable means of knowing that

their PII would not remain private and secure in Defendants' possession.

Fraudulent Conduct

163. Defendants' conduct is fraudulent in violation of the UCL because it is likely to deceive consumers.

164. Defendants' represent in their Privacy Policy that they safeguards consumers' sensitive personal information such as PII though it is in fact not safeguarded, as evident after the Data Breach.

165. Plaintiffs and the California Subclass members relied on Defendants' representations when they decided to utilize Defendants' services, something that they would not have done had they known their data would not be protected.

166. Thus, Defendants induced Plaintiffs and Class members to provide them with their PII.

167. Accordingly, Plaintiffs and the California Subclass members have suffered injury in fact, including lost money or property, as a direct and proximate result of Defendants' unlawful, unfair, and fraudulent acts. Absent these acts, Plaintiffs and the California Subclass members would not have purchased from Defendants.

168. Plaintiffs and California Subclass members have been harmed in the following ways: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) they suffered actual identity theft; (iv) their PII was improperly disclosed to unauthorized individuals; (v) the confidentiality of their PII has been breached; (vi) they were deprived of the value of their PII, for which there is a well-established national and international market; and/or (vii) they lost time and money to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

169. Plaintiffs seek appropriate relief under the UCL, including such orders as may be necessary: (a) to enjoin Defendants from continuing their unlawful, unfair, and

fraudulent acts or practices, and (b) to restore Plaintiffs and California Subclass members any money Defendants acquired by their unfair competition, including restitution. Plaintiffs also seek reasonable attorneys' fees and expenses under applicable law.

COUNT VII

VIOLATIONS OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT ("CLRA")

Cal. Civ. Code §§ 1750–1785

(Plaintiffs Individually and on Behalf of the California Subclass)

170. Plaintiffs reallege and incorporate by reference all preceding allegations as though fully set forth herein.

171. Defendants are "person(s)" as defined under the CLRA. *See* Cal. Civ. Code § 1761(c).

172. Plaintiffs and California Subclass members are "consumers" as defined under the CLRA. *See* Cal. Civ. Code § 1761(d).

173. Plaintiffs and Defendants engaged in "transactions" as defined under the CLRA when they engaged in activities related to the sale and purchase of tickets on Ticketmaster.com, or through other methods of purchase as provided by Defendant Ticketmaster. *See* Cal. Civ. Code § 1761(e).

174. The CLRA prohibits "unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer . . ." Cal. Civ. Code § 1770(a).

175. As alleged throughout this Complaint, Defendants engaged in unfair and deceptive acts in violation of the CLRA in transacting with Plaintiffs and California Subclass members, and such conduct was likely to deceive consumers.

176. Defendants violated the CLRA by representing that they had adequate security measures in place to protect Plaintiffs and Class members sensitive information

including PII when they in fact did not, in violation of Cal. Civ. Code § 1770(a)(5).

177. Plaintiffs and Class members relied on Defendants' representations about their data security measures in the Privacy Policy and were induced to provide their PII to Defendants.

178. Defendants failed to implement adequate safeguards and improperly handled and stored Plaintiffs' and the California Subclass members' PII.

179. Plaintiffs and Class members PII has been compromised in the Data Breach.

180. As a direct and proximate result of Defendants' unfair and deceptive conduct, Plaintiffs and the California Subclass members have been harmed.

181. The unfair and deceptive conduct alleged herein presents an ongoing and serious threat to Plaintiffs and Class Members.

182. Plaintiffs and the California Subclass members have been harmed in the following ways: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) they suffered actual identity theft; (iv) their PII was improperly disclosed to unauthorized individuals; (v) the confidentiality of their PII has been breached; (vi) they were deprived of the value of their PII, for which there is a well-established national and international market; and/or (vii) they lost time and money to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

183. Pursuant to Cal. Civ. Code § 1780(a), Plaintiffs, individually and on behalf of the California Subclass, seek injunctive relief for Defendants' violation of the CLRA.

184. Plaintiffs and Class members will be irreparably harmed if injunctive relief is not granted.

185. Pursuant to Cal. Civ. Code § 1782(a), Plaintiffs sent a demand letter to Defendants contemporaneously with the filing of this Complaint notifying them of their CLRA violations and providing them with an opportunity to correct their business

practices. If Defendants do not correct their business practices, Plaintiffs reserve the right to amend the complaint to add claims for monetary relief, including for actual, restitutionary, and punitive damages under the CLRA.

186. Additionally, pursuant to Cal. Civ. Code §§ 1780 and 1781, Plaintiffs, individually and on behalf of the California Subclass, seek compensatory and punitive damages under the CLRA and to recover attorneys' fees and costs.

187. Plaintiff's CLRA venue declaration is attached hereto as Exhibit 1 in accordance with Cal. Civ. Code § 1780(d).

COUNT VIII

VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 ("CCPA")

Cal. Civ. Code §§ 1798.100 et seq

(Plaintiffs Individually and on Behalf of the California Subclass)

188. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

189. The CCPA was passed by the California Legislature in 2018 to give consumers more control over their sensitive information and require businesses such as Defendants that possess, store, and maintain sensitive information to implement reasonable security procedures and practices to safeguard that data. *See* Cal. Civ. Code § 1798.100(e).

190. Plaintiffs are "consumers" under the CCPA. *See* Ca. Civ. Code § 1798.140(g).

191. Defendants are "business(es)" under the CCPA. *See* Ca. Civ. Code § 1798.140(c).

192. Defendants have failed to implement adequate safeguards as required by the CCPA.

193. Cal. Civ. Code § 1798.150(a)(1) states: "Any consumer whose nonencrypted or nonredacted personal information, as defined 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.

194. Personal Information, or PII, is defined by the CCPA to include an individual's name in combination with an account number or debit card number with any required security or access code that would permit access to an individual's financial account. Cal. Civ. Code § 1798.150(a)(1); *see also* § 1798.81(d)(1)(A).

195. The information stolen in the Data Breach belonging to Plaintiffs and Class members is personal information as defined in the CCPA.

196. Defendants violated the CCPA by failing to implement reasonable security measures to protect Plaintiffs' and Class members' PII, and as a result the Data Breach occurred.

197. Plaintiffs are providing notice to Defendants as required under the CCPA to present them the opportunity to cure their ongoing violations of the CCPA as alleged herein. *See* § 1798.150(b)(1). If Defendants do not cure their violation within 30 days, Plaintiffs reserve the right to amend this Complaint to add claims for monetary relief, including actual or statutory damages, or other monetary relief permitted under the CCPA. *See* § 1798.150(a)(1)(A).

198. Plaintiffs further seek injunctive and declaratory relief, attorneys' fees and costs, and all other relief available under the CCPA and that this Court deems just.

//

//

//

//

//

//

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

//

//

//

//

//

//

//

//

Dated: June 3, 2024

Respectfully submitted,

By: /s/ Steven A. Schwartz

STEVEN A. SCHWARTZ*
steveschwartz@chimicles.com
BEENA M. MCDONALD*
bmm@chimicles.com
ALEX M. KASHURBA*
amk@chimicles.com
MARISSA N. PEMBROKE*
mnp@chimicles.com
CHIMICLES SCHWARTZ KRINER
& DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500

JAMES J. ROSEMERGY*
jrosemergy@careydanis.com
CAREY, DANIS & LOWE
8235 Forsyth, Suite 1100
St. Louis, MO 63105
Telephone: (314) 725-7700

**pro hac vice* application to be submitted

By: /s/ David B. Jonelis

DAVID B. JONELIS (BAR NO. 265235)
djonelis@lavelysinger.com
LAVELY & SINGER PC
2049 Century Park East, Suite 2400
Los Angeles, California 90067-2906
Telephone: (310) 556-3501
Facsimile: (310) 556-3615

Attorneys for Plaintiffs and the Proposed Class

DEMAND FOR JURY TRIAL

Plaintiffs JODI CABALLERO, OWEN CONLAN, BRYAN CURTIS, KELLEY DAVIS, CHARLES FITZGERALD, BRENDAN HEALY, CHRIS RIPPEL, and MICHAEL WALTERS, individually and on behalf of all others similarly situated, demand a trial by jury.

Dated: June 3, 2024

Respectfully submitted,

By: /s/ Steven A. Schwartz

STEVEN A. SCHWARTZ*
steveschwartz@chimicles.com
BEENA M. MCDONALD*
bmm@chimicles.com
ALEX M. KASHURBA*
amk@chimicles.com
MARISSA N. PEMBROKE*
mnp@chimicles.com
CHIMICLES SCHWARTZ KRINER
& DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500

JAMES J. ROSEMERGY*
jrosemergy@careydanis.com
CAREY, DANIS & LOWE
8235 Forsyth, Suite 1100
St. Louis, MO 63105
Telephone: (314) 725-7700

**pro hac vice* application to be submitted

By: /s/ David B. Jonelis

DAVID B. JONELIS (BAR NO. 265235)
djonelis@lavelysinger.com
LAVELY & SINGER PC
2049 Century Park East, Suite 2400
Los Angeles, California 90067-2906
Telephone: (310) 556-3501
Facsimile: (310) 556-3615

Attorneys for Plaintiffs and the Proposed Class