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

SHANNON SPENCER, **GERRY MCAULEY**, and **RYAN JOSSART** individually and on behalf of all others similarly situated, Plaintiffs, v. **TICKETMASTER, LLC, and LIVE NATION ENTERTAINMENT, INC.**, Defendants.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Shannon Spencer, Gerry McAuley, and Ryan Jossart ("Plaintiffs"), individually and on behalf of all other similarly situated individuals (the "Class Members," as defined below), by and through their counsel, files this Class Action

Complaint against Ticketmaster, LLC and Live Nation Entertainment, Inc. ("Ticketmaster" or "Live Nation" or collectively "Defendants") and alleges the following based on personal knowledge of facts pertaining to themselves and on information and belief based on the investigation of counsel as to all other matters.

SUMMARY OF ACTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard personally identifiable information ("PII") of hundreds of millions of individuals, including but not limited to, names, contact information, and payment card information such as encrypted credit or debit card numbers and expiration dates (the "Data Breach").

2. Defendant Ticketmaster is the wholly owned subsidiary of Live Nation headquartered in West Hollywood, California. Defendant Ticketmaster is one of the largest ticket marketplaces in the world, specializing in sales, marketing, and distribution.[1]

3. Plaintiffs' and Class Members' sensitive personal information—which they entrusted to Defendants on the mutual understanding that Defendants would protect it against disclosure—was compromised and unlawfully exfiltrated due to the Data Breach.

[1] *See* https://www.livenation.com/ticketmaster/ (last visited July 7, 2024)

4. The PII compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target PII for its value to identity thieves. Even worse, hacking group, ShinyHunters, publicly confirmed it obtained the PII of hundreds of millions of Defendants' customers.[2] Further, ShinyHunters has also confirmed that it has posted the stolen data and has made it available for purchase for $500,000 in a "one-time sale".[3] According to ShinyHunters, the data stolen in the Data Breach is connected to over 500 million of Defendants' customers.[4]

5. As a result of the Data Breach, Plaintiffs and Class Members, suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII due to its theft and release for sale by hacking group, ShinyHunters; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and

[2] *See* https://completemusicupdate.com/ticketmaster-data-breach-new-details-emerge-from-official-filings/ (last visited July 7, 2024)
[3] *See* https://www.cbsnews.com/news/ticketmaster-breach-shinyhunters-560-million-customers/ (last visited July 7, 2024)
[4] *See* https://mashable.com/article/ticketmaster-data-breach-shinyhunters-hack (last visited July 7, 2024)

abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

6. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its customers' PII from a foreseeable and preventable cyber-attack.

7. Defendants maintained, used, and shared the PII in a reckless manner. In particular, the PII was used and transmitted by Defendants in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendants, and thus, Defendants were on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

8. Defendants disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

9. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct because the PII that Defendants collected and maintained is now in the hands of data thieves and is for sale to the public.

10. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

11. Plaintiffs and Class Members may also incur out of pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. Plaintiffs brings this class action lawsuit on behalf of all those similarly situated to address Defendants' inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information was stolen and released by cybercriminals in the Data Breach.

13. Through this Complaint, the Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was acquired during the Data Breach.

14. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from the Defendants, including the Plaintiffs.

16. This Court has personal jurisdiction over the Defendants because its principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

17. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendants' principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

PARTIES

18. Plaintiff Shannon Spencer is a resident and citizen of Anacortes, Washington. Mr. Spencer received the Notice Letter, via U.S. mail, directly from Defendant Ticketmaster, dated June 22, 2024.[5]

[5] *See* **Exhibit 1**.

19. Plaintiff Gerry McAuley is a resident and citizen of Puyallup, Washington. Mr. McAuley received the Notice Letter, via U.S. mail, directly from Defendant Ticketmaster, dated June 22, 2024.[6]

20. Plaintiff Ryan Jossart is a resident and citizen of Des Moines, Washington. Mr. Jossart received the Notice Letter, via U.S. mail, directly from Defendant Ticketmaster, dated June 22, 2024.[7]

21. Defendant Ticketmaster is the wholly owned subsidiary of Defendant Live Nation and is a limited liability company with its principal place of business in Hollywood, California.

22. Defendant Live Nation is a corporation incorporated in Delaware with its principal place of business in Beverly Hills, California.

FACTUAL ALLEGATIONS

Defendants' Business

23. Defendant Ticketmaster is a ticket management company for large-scale sports and entertainment, focusing on sales, marketing, and distribution.[8] Ticketmaster is the wholly owned subsidiary of Live Nation serving millions of customers within the United States and internationally.

[6] *See* **Exhibit 2**.
[7] *See* **Exhibit 3**.
[8] *See* https://www.livenation.com/ticketmaster/ (last visited July 7, 2024).

24. As a condition of receiving ticketing services, Plaintiffs and Class Members are required to provide their PII to Defendants, including their names, contact information, and payment card information such as encrypted credit or debit card numbers and expiration dates.

25. In the course of collecting PII from Plaintiffs and Class Members, Defendants promised to provide confidentiality and adequate security for customer data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

26. Indeed, the Privacy Statement posted on Defendant Ticketmaster's website promises to keep customer information safe, specifically stating that it has "security measures in place to protect your information."[9]

27. Plaintiffs and the Class Members relied on these promises and on this sophisticated business entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach

28. On or about June 22, 2024, Defendants began sending Plaintiffs and other Data Breach victims a Notice of Data Security Incident letter (the "Notice Letter"), informing them that:

[9] *See* https://privacy.ticketmaster.com/privacy-policy (last visited July 7, 2024),

> **What Happened**. Ticketmaster recently discovered that an unauthorized third party obtained information from a cloud database hosted by a third-party service provider. Based on our investigation, we determined that the unauthorized activity occurred between April 2, 2024 and May 18, 2024. On May 23, 2024, we determined that some of your personal information may have been affected by the incident. We have not seen any additional unauthorized activity in the cloud database since we began our investigation.
>
> **What Information Was Involved**. The personal information that may have been obtained by the third party may have included your name, basic contact information, and payment card information such as encrypted credit or debit card numbers and expiration dates.[10]

29. Nearly a month after Defendants notified Plaintiffs and Class Members of the Data Breach, hacking group, ShinyHunters, claimed responsibility for the Data Breach and is selling 1.3 terabytes worth of data stolen in the Data Breach for a one-time price of $500,000.[11]

30. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, when the Data Breach was discovered, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

31. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data

[10] *See* **Exhibit 1.**

[11] *See* https://mashable.com/article/ticketmaster-data-breach-shinyhunters-hack (last visited July 7, 2024)

Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

32. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

33. The attacker accessed and acquired files maintained by Defendants in a negligent manner.

34. Defendants had obligations created by the FTC Act, contract, common law, and industry standards to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

Data Breaches Are Preventable

35. Defendants could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

36. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

37. The unencrypted PII of Plaintiffs and Class Members is already on sale to the public on a popular hacking forum. Now, unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

38. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[12]

39. To prevent and detect cyber-attacks and/or ransomware attacks Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

[12] How to Protect Your Networks from RANSOMWARE, at 3, available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited July 7, 2024).

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[13]

[13] *Id*. at 3-4.

40. To prevent and detect cyber-attacks or ransomware attacks Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets
- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene
- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege
- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure
- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware

Scan Interface] for Office [Visual Basic for Applications].[14]

41. Given that Defendants were storing the PII of those who provided their information for ticketing services, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

42. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the publication of the PII of millions of individuals, including that of Plaintiffs and Class Members.

43. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendants Acquire, Collect, and Store Plaintiffs' and Class Members' PII

44. Defendants acquire, collect, and store a massive amount of PII in its ordinary course of business.

45. Defendants received Plaintiffs' and Class Members' PII in connection with providing ticketing services.

46. By obtaining, collecting, and using Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that

[14] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

47. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted it to Defendants absent a promise to safeguard that information.

48. Upon information and belief, in the course of collecting PII from Plaintiffs and Class Members, Defendants promised to provide confidentiality and adequate security for customer data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

49. Indeed, the Privacy Policy posted on Ticketmaster's website promises to keep customer information safe, specifically stating that it has "security measures in place to protect your information."[15]

50. Plaintiffs and the Class Members relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendants Knew, Or Should Have Known of the Risk Because Companies in Possession of PII Are Particularly Susceptible to Cyber Attacks

51. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee

[15] *See* https://privacy.ticketmaster.com/privacy-policy (last visited July 7, 2024).

Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

52. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

53. Additionally, as companies became more dependent on computer systems to run their business,[16] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[17]

54. Defendants knew and understood unprotected or exposed PII in the custody of institutions, like Defendants, is valuable and highly sought after by

[16] *See* Danny Brando, Implications of Cyber Risk for Financial Stability (May 12, 2022), available at: https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited July 7, 2024).

[17] *See* Dr. Suleyman Ozarslan, Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022 (March 24, 2022), available at: https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited July 7, 2024).

nefarious third parties seeking to illegally monetize that PII through unauthorized access.

55. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

56. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

57. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

58. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, use of that information and damage to victims may continue for years.

59. In the Notice Letter, Defendants makes an offer of 12 months of credit monitoring and credit score services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact that victims of data

breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII.

60. Defendants' offer of credit monitoring establishes that Plaintiffs' and Class Members' sensitive PII was in fact affected, accessed, compromised, exfiltrated from Defendants' computer systems, and released for sale by hacking gang, ShinyHunters.

61. Defendants knew, or should have known, the importance of safeguarding PII entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifying Information

62. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to

[18] 17 C.F.R. § 248.201 (2013).

identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[19]

63. The PII of individuals is 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.[20] For example, PII can be sold at a price ranging from $40 to $200.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

64. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

65. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when

---

[19] *Id*.

[20] 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 July 7, 2024).

[21] 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 July 7, 2024).

[22] https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited July 7, 2024).

it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

66. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

67. Moreover, the hacking group, ShinyHunters, has already published Plaintiffs' and Class Members' PII for sale to the public on a popular hacking website. As such, Plaintiffs and Class Members are at an imminent risk of future identity theft and fraud.

Defendants Failed to Comply with FTC Guidelines

68. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable

[23] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited July 7, 2024).

data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

69. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal consumer 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.[24]

70. 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.[25]

71. The FTC further recommends that companies not maintain 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

[24] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 7, 2024).
[25] *Id*.

security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

72. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

73. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

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

75. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

76. Upon information and belief, Defendants were at all times fully aware of its obligation to protect the PII of Plaintiffs and Class Members. Defendants were also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendants Failed to Comply with Industry Standards

77. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

78. Several best practices have been identified that, at a minimum, should be implemented by institutions in possession of PII, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

79. Other best cybersecurity practices that are standard for institutions include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting

up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

80. 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.

81. These foregoing frameworks are existing and applicable industry standards for software institutions, and upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries and Damages

82. As a result of Defendant's' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have

all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII and publishing of their PII for sale by hacking group, ShinyHunters; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

Data Breaches Increase Victims' Risk of Identity Theft

83. The unencrypted PII of Class Members has already ended up for sale to the public by criminal hackers.

84. In fact, the unencrypted PII of Plaintiffs and Class Members has already been published for sale by hacking group, ShinyHunters. The publication and release of Plaintiffs' and Class Members' PII creates an imminent threat of future identity theft and fraud.

85. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and

Class Members. Simply put, unauthorized individuals can easily access the PII of Plaintiffs and Class Members, especially considering it has already been released for sale to the public.

86. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

87. Plaintiffs' and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

88. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[26]

[26] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will

89. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII 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.

90. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still 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.

91. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like insurance information) of Plaintiffs and the other Class Members.

---

accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited July 7, 2024).

92. Thus, even if certain information (such as insurance information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

93. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate Risk of Identity Theft & Fraud

94. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

95. Thus, due to the actual and imminent risk of identity theft, Defendants, in its Notice Letter instructs Plaintiffs and Class Members to enroll in credit monitoring, remain vigilant for fraud and identity theft by reviewing account statements and credit reports, place a security freeze on credit files, report suspicious activity, and contact authorities.[27]

[27] *See* **Exhibit 1**.

96. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, contacting credit bureaus to place freezes on their accounts, and signing up for the credit monitoring and identity theft protection services offered by Defendant.

97. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28]

98. Plaintiffs' mitigation efforts are also consistent with the steps that the FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[29]

[28] United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/products/gao-07-737 (last visited July 7, 2024).

[29] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last visited July 7, 2024).

99. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

Diminution of Value of PII

100. PII is a valuable property right.[30] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond a doubt that PII has considerable market value.

101. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[31]

102. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[32]

---

[30] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report") (last visited July 7, 2024).

[31] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted) (last visited July 7, 2024).

[32] *See* Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited July 7, 2024).

103. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[33]

104. As a result of the Data Breach, Plaintiffs' 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 Plaintiffs 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.

105. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

106. The fraudulent activity resulting from the Data Breach may not come to light for years.

[33] *See* David Lazarus, Column: Shadowy data brokers make the most of their invisibility cloak, Los Angeles Times (Nov. 5, 2019), available at: https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited July 7, 2024).

107. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

108. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to millions of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

109. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

110. Given the type of targeted attack in this case, sophisticated criminal activity, the type of PII involved, entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

111. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her PII was

used to file unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

112. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

113. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach.

Plaintiff Shannon Spencer's Experience

114. Defendants obtained Plaintiff Spencer's PII in connection with providing him ticketing services.

115. At the time of the Data Breach, Defendants retained Plaintiffs' PII in its system.

116. Plaintiff Spencer is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendants had he known of Defendants' lax data security policies.

117. Plaintiff Spencer received the Notice Letter, by U.S. mail, directly from Ticketmaster, dated June 22, 2024. According to the Notice Letter, Plaintiffs' PII was improperly accessed and stolen by unauthorized third parties, including his name, basic contact information, and payment card information such as encrypted credit or debit card numbers and expiration dates.

118. As a result of the Data Breach, and at the direction of Defendants' Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach--valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

119. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and release of such PII for sale by hacking group, ShinyHunters; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to

access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

120. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

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

122. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

123. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Gerry McAuley's Experience

124. Defendants obtained Plaintiff McAuley's PII in connection with providing him ticketing services.

125. At the time of the Data Breach, Defendants retained Plaintiff's PII in its system.

126. Plaintiff McAuley is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendants had he known of Defendants' lax data security policies.

127. Plaintiff McAuley received the Notice Letter, by U.S. mail, directly from Ticketmaster, dated June 22, 2024. According to the Notice Letter, Plaintiff's PII was improperly accessed and stolen by unauthorized third parties, including his name, basic contact information, and payment card information such as encrypted credit or debit card numbers and expiration dates.

128. As a result of the Data Breach, and at the direction of Defendants' Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach–valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

129. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and release of such PII for sale by hacking group, ShinyHunters; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

130. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

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

132. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

133. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Ryan Jossart's Experience

134. Defendants obtained Plaintiff Jossart's PII in connection with providing him ticketing services.

135. At the time of the Data Breach, Defendants retained Plaintiff's PII in its system.

136. Plaintiff Jossart is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendants had he known of Defendants' lax data security policies.

137. Plaintiff Jossart received the Notice Letter, by U.S. mail, directly from Ticketmaster, dated June 22, 2024. According to the Notice Letter, Plaintiff's PII was improperly accessed and stolen by unauthorized third parties, including his name, basic contact information, and payment card information such as encrypted credit or debit card numbers and expiration dates.

138. As a result of the Data Breach, and at the direction of Defendants' Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach--valuable time

Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

139. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and release of such PII for sale by hacking group, ShinyHunters; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

140. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

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

142. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

143. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

144. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

145. The Class that Plaintiffs seek to represent is defined as follows:

Nationwide Class
All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the Data Breach (the "Class").

146. Excluded from the Class are the following individuals and/or entities: Defendants and Defendant's' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

147. Plaintiffs reserve the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

148. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. The Class is apparently identifiable within Defendants' records, and Defendants have already identified these individuals (as evidenced by sending them breach notification letters). It is believed that there are hundreds of millions of Class Members.

149. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

i. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class Members;

ii. Whether Defendants had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

iii. Whether Defendants had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

iv. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

v. Whether and when Defendants actually learned of the Data Breach;

vi. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

vii. Whether Plaintiffs' PII is for sale to the public;

viii. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

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

x. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

xi. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;

xii. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

150. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

151. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenges of these policies hinge on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

152. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

153. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

154. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed

is representative of that experienced by the Class and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

155. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

156. Adequate notice can be given to Class Members directly using information maintained in Defendant's' records.

157. Unless a Class-wide injunction is issued, Defendants may continue in its failure to properly secure the PII of Class Members, additional PII will be released for sale to the public and dark web, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

158. Further, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

159. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the

resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

i. Whether Defendants failed to timely notify the Plaintiffs and the class of the Data Breach;

ii. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

iii. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

iv. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

v. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PII; and

vi. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

160. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

161. Defendants gathered and stored the PII of Plaintiffs and Class Members as part of its ticketing services, which solicitations and services affect commerce.

162. Plaintiffs and Class Members entrusted Defendants with their PII with the understanding that Defendants would safeguard their information.

163. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

164. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it— to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of its security systems

in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

165. Defendants had a duty to employ reasonable security measures 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.

166. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks adequately protected the PII.

167. Defendant's' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII.

168. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

169. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

170. Defendants also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain pursuant to regulations.

171. Moreover, Defendants had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

172. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendants' possession might have been compromised, how it was compromised, precisely the types of data that were compromised and when, and whether additional PII is published for sale to the public or to the dark web. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

173. Defendants breached their duties, pursuant to the FTC Act and other applicable standards, 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:

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

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

iii. Allowing unauthorized access to Class Members' PII;

iv. Failing to detect in a timely manner that Class Members' PII had been compromised;

v. Failing to remove PII it was no longer required to retain pursuant to regulations;

vi. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

vii. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

174. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

175. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm this statute was intended to guard against.

176. Defendants' violation of Section 5 of the FTC Act constitutes negligence.

177. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

178. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

179. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in Defendants' industry.

180. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

181. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the

necessity for encrypting PII stored on Defendants' systems or transmitted through third party systems.

182. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members, including publication for sale by hacking group, ShinyHunters.

183. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

184. Defendants were in a position to protect against the harm suffered by the Plaintiffs and the Class as a result of the Data Breach.

185. Defendants' duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

186. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

187. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

188. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII and release and publication of such PII for sale by hacking group, ShinyHunters; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

189. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

190. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

191. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

192. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

193. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

194. Defendants breached its duties to Plaintiffs and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

195. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

196. Plaintiffs and Class Members are within the class of persons the FTC Act was intended to protect and the harm to Plaintiffs and Class Members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

197. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

198. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that the failure to meet its duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their PII.

199. Plaintiffs and Class Members were damaged as a result of Defendants' negligence, including having their PII released and published for sale by hacking group, ShinyHunters.

200. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

201. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

202. Plaintiffs and the Class entrusted their PII to Defendants. In so doing, Plaintiffs and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

203. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

204. Implicit in the agreement between Plaintiffs and Class Members and the Defendants to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their

PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

205. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendants, on the other, is demonstrated by their conduct and course of dealing.

206. Defendants solicited, offered, and invited Plaintiffs and Class Members to provide their PII as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their PII to Defendants.

207. In accepting the PII of Plaintiffs and Class Members, Defendants understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

208. On information and belief, at all relevant times Defendants promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

209. On information and belief, Defendants further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' PII would remain protected.

210. Plaintiffs and Class Members would not have entrusted their PII to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure.

211. Plaintiffs and Class Members would not have entrusted their PII to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

212. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

213. Defendants breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

214. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain. Specifically, Plaintiffs and Class Members were damaged as a result of Defendants' breach, including having their PII released and published for sale by hacking group, ShinyHunters.

215. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

216. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

217. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

218. Plaintiffs bring this Count in the alternative to the breach of implied contract count above.

219. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, Defendants and/or its agents were paid for Defendants' services and in so doing, Plaintiffs and Class Members also provided Defendants with their PII. In exchange, Plaintiffs and Class Members should have received from Defendants the services that were the subject of the transaction and should have had their PII protected with adequate data security.

220. Defendants knew that Plaintiffs and Class Members conferred a benefit upon it and have accepted and retained that benefit by accepting and

retaining the PII entrusted to it. Defendants profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' PII for business purposes.

221. Defendants failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided.

222. Defendants acquired the PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

223. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have entrusted their PII to Defendants.

224. Plaintiffs and Class Members have no adequate remedy at law.

225. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

226. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII and release of such PII for sale to the public by hacking group, ShinyHunters; (iii) lost or diminished value of PII; (iv) lost time

and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

227. Plaintiffs 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 its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

228. Plaintiffs 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 V
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
CAL. BUS. & PROF. CODE § 7200, *et seq.*
(On Behalf of Plaintiffs and Class Members)

229. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein.

230. Defendants' acts and omissions as alleged herein emanated and were directed from California.

231. By reason of the conduct alleged herein, Defendants engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

232. Defendants stored the PII of Plaintiffs and Class Members in its computer systems.

233. Defendants knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations that would have kept Plaintiffs' and Class Members' PII secure and prevented the loss or misuse of that PII.

234. Defendants did not disclose at any time that Plaintiffs' and Class Members' PII was vulnerable to hackers because Defendants' data security measures were inadequate and outdated, and Defendants were the only ones in possession of that material information, which Defendants had a duty to disclose.

Unlawful Business Practices

235. As noted above, Defendants violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, by omission, the safety of its computer systems, specifically the security thereof, and its ability to safely store Plaintiffs' and Class Members' PII.

236. Defendants also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security.

237. If Defendants had complied with these legal requirements, Plaintiffs and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendants' failure to timely notify Plaintiffs and Class Members of the Data Breach.

238. Defendants' acts and omissions as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the FTC Act.

239. Plaintiffs and Class Members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices. In addition, Plaintiffs' and Class Members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection

services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Unfair Business Practices

240. Defendants engaged in unfair business practices under the "balancing test." The harm caused by Defendants' actions and omissions, as described in detail above, greatly outweighs any perceived utility. Indeed, Defendants' failure to follow basic data security protocols and failure to disclose the inadequacies of Defendants' data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiffs and Class Members, directly causing the alleged harm.

241. Defendants engaged in unfair business practices under the "tethering test." Defendants' actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a

matter of statewide concern."). Defendants' acts and omissions thus amount to a violation of the law.

242. Defendants engaged in unfair business practices under the "FTC test." The harm caused by Defendants' actions and omissions, as described in detail above, is substantial in that it affects millions of Class Members and has caused those persons to suffer actual harm. Such harms include a substantial risk of identity theft, disclosure of Plaintiffs' and Class Members' PII to third parties without their consent, diminution in value of their Personal Information, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiffs' and Class Members' PII remains in Defendants' possession, without adequate protection, and is also in the hands of hacking group, ShinyHunters. Defendants' actions and omissions violated Section 5(a) of the Federal Trade Commission Act. See 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g.*, *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated §5(a) of FTC Act).

243. Plaintiffs and Class Members suffered injury in fact and lost money or property as the result of Defendants' unfair business practices. Plaintiffs' and Class Members' PII was taken and in the hands of those who will use it for their own advantage, and is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and Class Members have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

244. As a result of Defendants' unlawful and unfair business practices in violation of the UCL, Plaintiffs and Class Members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grants the following:

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

vi. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vii. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendants to segment data by, among other things, creating firewalls and controls so that if one area of

Defendants' network is compromised, hackers cannot gain access to portions of Defendants' systems;

xi. requiring Defendants to conduct regular database scanning and securing checks;

xii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xiii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance

with Defendants' policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xviii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to

provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: July 9, 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

William B. Federman*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120

Telephone: (405) 235-1560
-and-
212 W. Spring Valley Road
Richardson, TX 75081

*Pro Hac Vice forthcoming

Counsel for the Plaintiffs and the Proposed Class