IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

CHASTINE DICKEY-JOHNSON, and SERENA CHAPMAN, individually and on behalf of all others similarly situated, ***Plaintiffs*,** vs. **TICKETMASTER, LLC, and LIVE NATION ENTERTAINMENT, INC.** ***Defendants*.**	**Civil Action No. 2:24-cv-2623** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Chastine Dickey-Johnson, and Serena Chapman ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Ticketmaster, LLC and Live Nation Entertainment, Incorporated (collectively, "Defendants") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to Plaintiffs' own actions and to counsels' investigation, and upon information and belief as to all other matters, as follows:

SUMMARY OF ACTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard the personally identifiable information (PII) of its customers, including, but not limited to: full names, addresses, email addresses, phone numbers and credit card details.

2. Ticketmaster, LLC ("Ticketmaster") is one of the largest ticket sales and distribution companies in the world. Ticketmaster operates a digital ticketing platform that requires customers to provide their PII prior to purchase. Upon information and belief, in February 2009, Ticketmaster entered into an agreement to merge with event promoter Live Nation to form Live

Nation Entertainment, Incorporated ("Live Nation"). Together, Defendants promote, operate, and manage entertainment venues and ticket sales for live entertainment events.

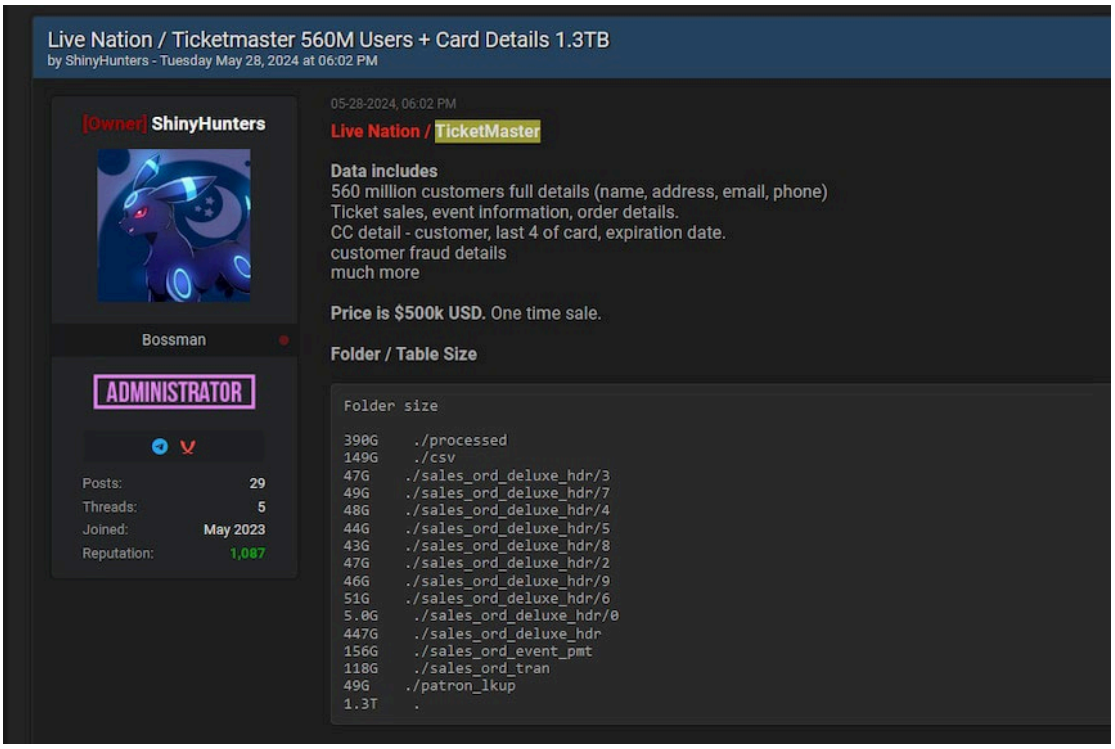
3. On, or about, May 20, 2024, Plaintiffs' and Class Members' personal information—which they entrusted to Defendants on the mutual understanding that Defendants would protect it against unauthorized disclosure—was compromised in a data breach (hereafter referred to as, the "Data Breach").[1]

4. The Data Breach included personal details of about 560 million Ticketmaster customers.[2] The PII compromised in the Data Breach was exfiltrated by cyber-criminals who target PII for its value to identity thieves.

5. ShinyHunters, the group claiming responsibility for the Data Breach, has been linked to a string of high-profile data breaches resulting in millions of dollars in losses.[3]

6. The hackers are demanding a ransom payment of $500,000.00 to prevent the data from being resold on the dark web; a clear indication that the data breach was for the purpose of using the Plaintiffs' and Class Members' personal information to perpetuate identity theft and other fraud.[4]

[1] *Live Nation Entertainment Form 8-K,* https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm (accessed June 11, 2024).
[2] *Data allegedly stolen from 560 million Ticketmaster users*, https://www.bbc.com/news/articles/c899pz84d8zo (accessed June 11, 2024).
[3] *Id.*
[4] *Id*.



**Screenshot of ShinyHunters advertising the sale of Ticketmaster customer PII on the dark web.*

7. The invasion of the Plaintiffs' and Class Members' privacy suffered in this Data Breach constitutes an injury in fact. Additionally, the Plaintiffs and Class Members are at an increased risk of future harm, including identity theft, fraud, spam, phishing, or other impersonation attacks.

8. There is a substantial risk of future identity theft or fraud where the Plaintiffs' and Class Members' PII was targeted by a sophisticated hacker group (ShinyHunters), known for stealing and reselling as much personal and financial data as they can.[5] Furthermore, since 2020, ShinyHunters has stolen over 900 million customer records in a series of high-profile data breaches (e.g., GitHub, AT&T, Pizza Hut). Upon information and belief, ShinyHunters has accumulated

[5] *What we know about the 'remarkably devious' ShinyHunters hackers allegedly behind the Ticketmaster data leak*, https://www.abc.net.au/news/2024-05-31/shinyhunters-cyber-hackers-ticketmaster-data-breach/103911928 (accessed June 11, 2024).

enough personal information from that series of data breaches to be able to open a bank account or commit other fraud using stolen identities.

9. Plaintiffs and Class Members face a substantial risk of future spam, phishing, or other social engineering attacks where their full names, addresses, email addresses, and phone numbers were stolen by a hacker group (ShinyHunters), known for stealing and reselling personal data. For example, once a cybercriminal has sold a stolen email address or phone number, that email address or phone number is sent spam messages that are "carefully calculated to get the recipient to click on a link that infects a computer with malware."[6] Once the computer is infected with malware, the computer is locked down and the user is sent a ransom demand, which must be paid to regain access to the computer.

10. As a result of the Data Breach, Plaintiffs and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (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) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendants' possession or control and is subject to further unauthorized disclosures so long as Defendants fail to implement appropriate and reasonable measures to protect the PII.

[6] *Id.*

11. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable data protection procedures, including vendor management, necessary to protect consumers' PII from a foreseeable and preventable risk of unauthorized disclosure.

12. 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 the data in a dangerous condition.

13. 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, or the data systems of its vendors, 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. Plaintiffs and Class Members are now at risk because of Defendants' wrongful conduct.

14. Armed with the PII acquired in the Data Breach, data thieves have already engaged in identity theft and fraud and can, in the future, commit a variety of crimes including, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

15. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a substantial 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. Plaintiffs and Class Members may also incur out of pocket costs, for purchasing credit monitoring services, credit

freezes, credit reports, or other protective measures to deter and detect identity theft. Plaintiffs and Class Members may also incur out of pocket costs, for purchasing products to protect themselves from spam emails, phone calls, and text messages.

16. Plaintiffs bring this class action lawsuit on behalf 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 had been disclosed to an unauthorized third party and precisely what information was accessed.

17. Through this Complaint, Plaintiffs seek to remedy these harms individually, and on behalf of all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiffs and Class Members have a continuing interest in ensuring that their personal information is kept confidential and protected from disclosure, and they should be entitled to injunctive and other equitable relief.

JURISDICTION & VENUE

18. 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 $5,000,000.00, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiffs, is a citizen of a state different from Defendants.

19. This Court has personal jurisdiction over Defendants because their principal place of business is in this District. Defendants have also purposefully availed themselves of the laws, rights, and benefits of the State of Pennsylvania.

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

PARTIES

21. Plaintiff Chastine Dickey-Johnson is a citizen of the State of North Carolina. At all relevant times, Plaintiff Dickey-Johnson has been a resident of Indian Trail, North Carolina.

22. Plaintiff Serena Chapman is a citizen of the State of Texas. At all relevant times, Plaintiff Chapman has been a resident of San Antonio, Texas.

23. Defendant Live Nation Entertainment Incorporated, maintains a principal place of business at 334 South Street, Philadelphia, Pennsylvania 19147. Live Nation produces live concerts and offers digital ticketing services for leading arenas, stadiums, professional sports franchises and leagues, college sports teams, performing arts venues, museums, and theaters around the world. Live Nation provides ticketing solutions through websites, mobile apps, retail outlets and call centers.

24. Defendant Ticketmaster, LLC, is a wholly owned subsidiary of Defendant Live Nation Entertainment, Incorporated, with a principal place of business located at 1020 Pattison Avenue, Philadelphia, Pennsylvania 19148. Ticketmaster operates as a ticket distribution company; it buys, transfers, and sells tickets for live music, sporting, arts, theater, and family events around the around the world.

FACTUAL ALLEGATIONS

25. Defendants promote, operate, and manage entertainment venues and ticket sales for live entertainment events. Defendants permit users to buy and sell tickets online for concerts, sports, theater, family, and other events using the website www.ticketmaster.com.

26. Plaintiffs and Class Members are current and former customers of Ticketmaster and have used, or created accounts on, ticketmaster.com.

27. In the course of their relationship, customers, including Plaintiffs and Class Members, provided Defendants with at least the following: full names, dates of birth, contact information, and credit card, debit card, or banking information.

28. Upon information and belief, while collecting PII from customers, including Plaintiffs, Defendants promised to provide security measures to protect customer information. When customer data is transferred to a third-party, Defendants promised to "ensure that appropriate safeguards are put in place" to ensure customer data is "protected to the highest standard."[7] More specifically, when personal information is transferred to a third party, Defendants represented that they would "use contractual measures and internal mechanisms requiring the recipient to comply with the privacy standards of the exporter."[8] These promises were contained in the applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

29. Plaintiffs and the Class Members, as customers of Defendants, relied on these representations and on these sophisticated business entities 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.

30. On May 20, 2024, Live Nation identified unauthorized activity within a third-party cloud database environment containing personal data (primarily from its Ticketmaster L.L.C. subsidiary).[9] On May 27, 2024, Live Nation discovered that the personal details of about 560

[7] *Ticketmaster Privacy Policy*, https://privacy.ticketmaster.com/privacy-policy (accessed June 11, 2024).
[8] *Id.*
[9] *Live Nation Entertainment SEC Form 8-K,* https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm (accessed June 11, 2024).

million Ticketmaster customers—including Plaintiffs and Class Members—was exfiltrated by cyber-criminals demanding a ransom payment of $500,000.00 to prevent the data from being resold on the dark web.

31. Information disclosed by ShinyHunters, the cyber-criminals responsible for the Data Breach, indicates the stolen information includes "a treasure trove of sensitive user information, including full names, addresses, email addresses, phone numbers, ticket sales and event details, order information, and partial payment card data."[10]

32. With the information that was accessed in the Data Breach, "cybercriminals can commit identity theft and financial fraud, launch phishing attacks, or take over online accounts. They may also use the data for blackmail, extortion, medical identity theft or credential stuffing which could lead to significant financial losses for customers, [and] damage to credit scores."[11]

33. Data stolen in the Data Breach included unencrypted customer data that had been shared or stored with a third-party cloud database vendor. Plaintiffs further believe that their PII and that of the Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of the ShinyHunters group and other cybercriminals that commit cyber-attacks of this type.

34. Defendants collect, and sell the PII of its customers, former customers, and other personnel. Defendants collect personal information when a customer buys merchandise or a ticket to an event. Defendants then sell personal information like names, physical addresses, phone numbers, email addresses, IP addresses, information about transactions, preferences, and attributes, cookies and device attributes to business partners, data brokers, and service providers.[12]

---

[10] *Hackers Claim Ticketmaster Data Breach: 560M Users' Info for Sale at $500K*, https://hackread.com/hackers-ticketmaster-data-breach-560m-users-sale (accessed June 11, 2024).
[11] *Id*.
[12] *Ticketmaster Privacy Policy*, https://privacy.ticketmaster.com/privacy-policy (accessed June 11, 2024).

35. By obtaining, collecting, and using Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

36. 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. Indeed, Defendants make the following representations to customers on their ticketmaster.com website:

a. "The security of our fans' information is a priority for us."
b. "We take all necessary security measures to protect personal information that's shared and stored with us."
c. "We work with our partners to put on amazing live events and provide additional services that we think you'll love. We always ask them to maintain the same standards of privacy."
d. "We embed privacy in the development of our products and services to ensure that we always respect your personal information."
e. "As an international company, no matter where you are located, our control framework is built around global data protection laws."
f. "We comply with all applicable data protection laws and listen to your expectations when it comes to how your information is handled."
g. "We have a global privacy team of trust and security professionals that ensure end-to-end protection of your personal information throughout the data lifecycle."[13]

37. Plaintiffs and the Class Members relied on Defendants to keep their PII confidential and securely maintained, to ensure that third-party vendors adhered to reasonable security measures, to use this information for business purposes only, and to permit only authorized uses and disclosures of this information.

38. Defendants' representations about their commitment to security and confidentiality of the personal information they collect and share with third parties was false or misleading as an

[13] *Ticketmaster Commitments*, https://privacy.ticketmaster.com/our-commitments (accessed June 11, 2024).

unauthorized person was able to access and exfiltrate personal data from one of Defendants' cloud database vendors. Defendants have failed to maintain the confidentiality and security of Plaintiffs' and the Class Members' PII and/or failed to take reasonable steps to protect Plaintiffs' and the Class Members' PII from disclosure.

Data Breaches Are Avoidable

39. Upon information and belief, the Data Breach was a direct result of Defendants' failure to implement adequate and reasonable data protection procedures, including vendor management, necessary to protect Plaintiffs' and Class Members' PII from a foreseeable and preventable risk of unauthorized disclosure.

40. Upon information and belief, the Data Breach occurred as the result of a ransomware attack. In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and then demand payment to restore control over the network.[14] Ransomware groups frequently implement a double extortion tactic, where the cybercriminal posts portions of the data to increase their leverage and force the victim to pay the ransom, and then sells the stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[15]

41. 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:

[14] *Ransomware FAQs*, https://www.cisa.gov/stopransomware/ransomware-faqs (accessed June 11, 2024).
[15] *Ransomware: The Data Exfiltration and Double Extortion Trends*, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (accessed June 11, 2024).

Preventative Measures

a. 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.

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email.

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

d. Configure firewalls to block access to known malicious IP addresses.

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

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

g. 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.

h. 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.

i. 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.

j. 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.

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

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

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

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

o. Conduct an annual penetration test and vulnerability assessment.

p. Secure your backups.[16]

q. Identify the computers or servers where sensitive personal information is stored.

[16] *How to Protect Your Networks from Ransomware*, at p.3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (accessed June 11, 2024).

r. Identify all connections to the computers where you store sensitive information. These may include the internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, digital copiers, and wireless devices like smartphones, tablets, or inventory scanners.

s. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.

t. Don't store sensitive consumer data on any computer with an internet connection unless it's essential for conducting your business.

u. Encrypt sensitive information that you send to third parties over public networks (like the internet) and encrypt sensitive information that is stored on your computer network, laptops, or portable storage devices used by your employees. Consider also encrypting email transmissions within your business.

v. Regularly run up-to-date anti-malware programs on individual computers and on servers on your network.

w. Check expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities and implement policies for installing vendor-approved patches to correct problems.

x. Restrict employees' ability to download unauthorized software. Software downloaded to devices that connect to your network (computers, smartphones, and tablets) could be used to distribute malware.

y. Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems.

z. To detect network breaches when they occur, consider using an intrusion detection system.

aa. Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities.

bb. Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate.

cc. Teach employees about the dangers of spear phishing—emails containing information that makes the emails look legitimate. These emails may appear to come from someone within your company, generally someone in a position of authority. Make it office policy to independently verify any emails requesting sensitive information.

dd. Before you outsource any of your business functions investigate the company's data security practices and compare their standards to yours.[17]

42. Defendants' security practices were ineffective since Defendants did not ensure their third-party vendors were responsible for implementing them. When a vendor is using, collecting, or storing personal data, the following are common data protection requirements:

Vendor Management

a. Require the vendor to impose technical and organizational measures to protect personal data, similar to those listed above.
b. Ensure that the vendor requires each individual processing the personal data to be subject to a duty of confidentiality.
c. Require the vendor (and any subcontractors) to comply with all applicable statutes and data protection obligations as the Defendants.
d. Require the vendor to cooperate with reasonable privacy assessments and security audits.
e. Prohibit the vendor from retaining, using, or disclosing personal data for any purpose other than the specified business purpose.
f. Require the vendor to notify the Defendants of a data breach or after vendor makes a determination that it can no longer meet its data protection obligations.
g. Require the vendor to provide timely notice to individuals impacted by a data breach event.

43. Given that Defendants stored the PII of its current and former customers, Defendants could and should have implemented all the above measures to prevent and detect cyberattacks. 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 exposure of Plaintiffs' and the Class members' PII.

44. Defendants knew and understood unencrypted PII is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII. At all relevant times,

[17] *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (accessed June 11, 2024).

Defendants knew, or reasonably should have known, of the importance of safeguarding customer PII and of the foreseeable consequences that would occur if Defendants' network (or the network of their vendors) was breached, including the significant cost that would be imposed on Plaintiffs and the Class Members as a result.

45. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records. The Class is incurring and will continue to incur such damages in addition to any harms associated with the fraudulent use of their PII.

46. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures.

47. Personal identifying information is of great value to criminals. Data such as name, address, phone number, and credit history has been sold at prices ranging from $40 to $200 per record.[18]

48. Given these facts, by transacting business with Plaintiffs and Class Members, collecting and selling their PII, using their PII to market additional products and services to them, and then compromising the privacy of their PII has deprived Plaintiffs and Class Members of the benefit of their bargain with Defendants.

49. The invasion of the Plaintiffs' and Class Members' privacy suffered in this Data Breach constitutes an injury in fact. Additionally, the Plaintiffs and Class Members are at an increased risk of future harm, including identity theft, fraud, spam, phishing, or other impersonation attacks.

50. There is a substantial risk of future identity theft or fraud where the Plaintiffs' and Class Members' PII was targeted by a sophisticated hacker group (ShinyHunters), known for

[18] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymousbrowsing/in-the-dark/

stealing and reselling as much personal and financial data as they can.[19] Furthermore, since 2020, ShinyHunters has stolen over 900 million customer records in a series of high-profile data breaches (*e.g.*, GitHub, AT&T, Pizza Hut). Upon information and belief, ShinyHunters has accumulated enough personal information from that series of data breaches to be able to open a bank account or commit other fraud using stolen identities.

51. Plaintiffs and Class Members face a substantial risk of future spam, phishing, or other social engineering attacks where their full names, addresses, email addresses, and phone numbers were stolen by a hacker group known for selling personal data on the dark web.

52. As a result of the Data Breach, Plaintiffs and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (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) experience an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendants' possession or control and is subject to further unauthorized disclosures so long as Defendants fail to implement appropriate and reasonable measures to protect the PII.

53. As a result of the Data Breach, unauthorized individuals can easily access the PII of Plaintiffs and Class Members. 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

[19] *What we know about the 'remarkably devious' ShinyHunters hackers allegedly behind the Ticketmaster data leak*, https://www.abc.net.au/news/2024-05-31/shinyhunters-cyber-hackers-ticketmaster-data-breach/103911928 (accessed June 11, 2024).

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.

54. 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.

55. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[20] 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.

56. Since 2020, ShinyHunters has stolen over 900 million customer records in a series of high-profile data breaches (e.g., GitHub, AT&T, Pizza Hut). The development of "Fullz" packages is highly likely considering the volumes of data acquired by ShinyHunters. In other words, even if certain information such as social security numbers were not included in the PII that was exfiltrated in the Data Breach, criminals can easily create a Fullz package and either sell the information to the highest bidder or use the complete profile to perpetuate fraud or theft.

[20] "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 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://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texaslife-insurance.

57. 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 and signing up for the credit monitoring and identity theft protection services.

58. Plaintiffs' mitigation efforts are also consistent with the several steps that the FTC recommends that data breach victims take 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.[21]

59. PII is a valuable property right. For example, sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[22] In 2019, the data brokering industry was worth roughly $200 billion.[23]

60. 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.

61. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of PII involved, there is a strong probability that entire batches of stolen information have

---

[21] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

[22] *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).

[23] *Column: Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers

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.

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

63. 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 protect Class Members from the risk of identity theft that arose from the Data Breach.

64. Furthermore, Defendants' poor data security practices deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendants for products or services, customers understood and expected that they were, in part, paying for the protection of their personal data, when in fact, Defendants did not provide adequate security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

CLASS ALLEGATIONS

65. Plaintiffs brings 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.

66. The Class that Plaintiffs seeks to represent is defined as follows:

Nationwide Class

All individuals residing in the United States whose PII was accessed and acquired by an unauthorized party as a result of a data breach that occurred on, or about, May 20, 2024, as reported by Defendant Live Nation (the "Class").

North Carolina Subclass

All individuals residing in North Carolina whose PII was accessed and acquired by an unauthorized party as a result of the Data Breach as reported by Defendant Live Nation (the "North Carolina Subclass").

Texas Subclass

All individuals residing in Texas whose PII was accessed and acquired by an unauthorized party as a result of the Data Breach as reported by Defendant Live Nation (the "Texas Subclass").

67. Collectively, the Class, Texas Subclass, and North Carolina Subclass are referred to as the "Classes" or "Class Members."

68. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' 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.

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

70. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time and such number is exclusively in the possession of Defendants, upon information and belief, millions of individuals were impacted in Data Breach.

71. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. Among the

questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, including the following:

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

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

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

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

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

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

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

h. 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;

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

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

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

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

73. 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 Classes, 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 Classes as a whole. Defendants' policies challenged herein apply to and affect Class

Members uniformly and Plaintiffs' challenges of these policies hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

74. 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 seeks 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.

75. 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.

76. 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 Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

77. 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 demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

78. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

79. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Classes, 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.

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

81. 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:

a. Whether Defendants failed to timely notify the Plaintiffs and the Classes of the Data Breach;

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

c. Whether Defendants' (or their vendors') security measures to protect their network were reasonable in light of industry best practices;

d. Whether Defendants' (or their vendors') failure to institute adequate data protection measures amounted to negligence;

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

f. Whether Defendants made false representations about their data privacy practices and commitment to the security and confidentiality of customer information; and

g. Whether adherence to FTC recommendations for protecting personal information would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT 1: NEGLIGENCE
(On Behalf of the Plaintiffs and the Classes)

82. Plaintiffs re-allege and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

83. Defendants require their customers, including Plaintiffs and Class Members, to submit non-public PII in the ordinary course of providing ticketing services for live entertainment events.

84. Defendants gathered and stored the PII of Plaintiffs and Class Members as part of their business of soliciting its services to their customers. Plaintiffs and Class Members entrusted Defendants with their PII with the understanding that Defendants would adequately safeguard their information.

85. Defendants had full knowledge of the types of PII they collect and the types of harm that Plaintiffs and Class Members would suffer if that data was accessed and exfiltrated by an unauthorized third-party.

86. By collecting, storing, sharing, and using the Plaintiffs' and Class Members' PII for commercial gain, Defendants assumed a duty to use reasonable means to safeguard the personal data they obtain.

87. Defendants' duty included a responsibility to ensure its vendors: (i) implemented reasonable measures to detect and prevent unauthorized intrusions into their network; (ii) were contractually obligated to adhere to the requirements of Defendants' privacy policy; (iii) were required to comply with the same statutes and data protection obligations as the Defendants; (iv) were required to submit to regular privacy assessments and security audits; (v) were regularly audited for compliance with contractual and other applicable data protection obligations; and, (vi) were obligated to provide timely notice to individuals impacted by a data breach event.

88. 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 or deceptive practices that affect commerce. Deceptive practices, as interpreted and enforced by the FTC, include failing to adhere to a company's own stated privacy policies.

89. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII they were no longer required to retain. Defendants had a duty to promptly and adequately notify Plaintiffs and the Classes of the Data Breach.

90. Defendants have a duty to adequately disclose that the PII of Plaintiffs and the Classes within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

91. 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:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
b. Failing to adequately monitor the security of their networks and systems;
c. Allowing unauthorized access to Class Members' PII;
d. Failing to detect in a timely manner that Class Members' PII had been compromised;
e. Failing to remove former customers' PII it was no longer required to retain;
f. 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,
g. Failing to ensure their vendors implemented data security practices consistent with Defendants' published privacy policies.

92. 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 the statue was intended to guard against.

93. The injuries resulting to Plaintiffs and the Classes because of Defendants failure to use adequate security measures was reasonably foreseeable. Further, the Data Breach was reasonably foreseeable given the Defendants prior experience with cyberattacks and data breaches.

94. Plaintiffs and the Class were the foreseeable victims of a data breach. Defendants knew or should have known of the inherent risks in collecting and storing PII, the critical importance of protecting that PII, and the necessity of protecting PII transmitted to and maintained on third party systems.

95. Plaintiffs and the Classes had no ability to protect the PII in Defendants' possession. Defendants were in the best position to protect against the harms suffered by Plaintiffs and the Classes as a result of the Data Breach.

96. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Classes, their PII would not have been compromised. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Classes and the harm, or risk of imminent harm, suffered by Plaintiffs and the Classes.

97. As a result of the Data Breach, Plaintiffs and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (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) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendants' possession or control and is subject to further unauthorized disclosures so long as Defendants fail to implement appropriate and reasonable measures to protect the PII.

98. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Classes have suffered and will suffer the continued risks of exposure of their PII, which remain 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 in its continued possession.

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

100. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data protection procedures; (ii) require vendors to submit to annual audits of their systems and protection procedures; and (iii) to provide adequate credit monitoring to all Class Members.

COUNT 2: NEGLIGENCE *PER SE*
(On Behalf of the Plaintiffs and the Classes)

101. Plaintiffs reallege and incorporates by reference all the allegations contained in the foregoing paragraphs, as if fully set forth herein.

102. 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 or deceptive practices that affect commerce. Deceptive practices, as interpreted and enforced by the FTC, include failing to adhere to a company's own stated privacy policies.

103. Defendants violated Section 5 of the FTC Act by failing to adhere to its own Privacy Policy regarding the confidentiality and security of Plaintiffs and Class Members information. Defendants further violated Section 5 of the FTC Act, and other state consumer protection statutes by failing to use reasonable measures to protect PII.

104. Defendants' violations of Section 5 of the FTC Act, and other state consumer protection statutes, constitutes negligence *per se.*

105. Plaintiffs and Class Members are within the class of persons Section 5 of the FTC Act, and other state consumer protection statutes, were intended to protect. Moreover, the harm that has occurred is the type of harm the FTC Act, and similar state statutes were intended to guard against.

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

107. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (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) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendants' possession or control and is subject to further unauthorized disclosures so long as Defendants fail to implement appropriate and reasonable measures to protect the PII.

108. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Classes have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

109. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Classes have suffered and will suffer the continued risks of exposure of their PII, which remain 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 in its continued possession.

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

111. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data protection procedures; (ii) require vendors to submit to annual audits of their systems and protection procedures; and (iii) to provide adequate credit monitoring to all Class Members.

COUNT 3: BREACH OF IMPLIED CONTRACT
(On Behalf of the Plaintiffs and the Classes)

112. Plaintiffs reallege and incorporates by reference all the allegations contained in the foregoing paragraphs, as if fully set forth herein.

113. Defendants require their customers, including Plaintiffs and Class Members, to submit non-public PII in the ordinary course of providing ticketing services for live entertainment events.

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

115. Defendants promulgated, adopted, and implemented written privacy policies whereby they promised Plaintiffs and Class Members that they would (a) use 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 notice of any unauthorized access and/or theft of their PII, (e) reasonably ensure their vendors safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

116. Plaintiffs and Class Members would not have entrusted their PII to Defendants in the absence of their implied promise to implement reasonable data protection measures.

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

118. Defendants breached the implied contracts it made with Plaintiffs and the Classes by failing to protect their personal information, by failing to delete the information once the relationship ended, and by failing to provide adequate notice of the Data Breach.

119. 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.

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

121. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data protection procedures; (ii) require vendors to submit to annual audits of their systems and protection procedures; and (iii) to provide adequate credit monitoring to all Class Members.

COUNT 4: UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Classes)

122. Plaintiffs reallege and incorporate by reference all the allegations contained in the foregoing paragraphs, as if fully set forth herein.

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

124. By providing their PII, Plaintiffs and Class Members conferred a monetary benefit on Defendants. Defendants knew that Plaintiffs and Class Members conferred a benefit upon them

and have accepted and retained that benefit. Defendants sold their PII and used the data to market and sell additional services to Plaintiffs and Class Members.

125. 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.

126. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, they would not have entrusted their PII to Defendants.

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

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

129. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (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) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendants' possession or control and is subject to further unauthorized disclosures so long as Defendants fail to implement appropriate and reasonable measures to protect the PII.

130. 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 their wrongful conduct.

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 Classes, and appointing Plaintiffs and her Counsel to represent the Classes;

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 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 acts described herein;

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

iii. requiring Defendants to delete the PII of Plaintiffs and Class Members unless Defendants can provide a 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 implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII they collect; and

v. requiring Defendants to audit, test, and train their vendors regarding data protection procedures.

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: June 14, 2024

Respectfully Submitted,

By: */s/ Gary F. Lynch*
Gary F. Lynch (PA 56887)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Fax: (412) 231-0246
Email: Gary@lcllp.com

-AND-

By: */s/ Paul J. Doolittle*
Paul J. Doolittle (*Pro Hac Vice* Forthcoming)
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
cmad@poulinwilley.com

Attorneys for Plaintiffs

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

CHASTINE DICKEY-JOHNSON, and SERENA CHAPMAN

(b) County of Residence of First Listed Plaintiff Union, NC
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Lynch Carpenter, LLP, 1133 Penn Avenue, 5th Floor, Pittsburgh, PA 15222. T: (412) 322-9243

DEFENDANTS

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

County of Residence of First Listed Defendant Philadelphia, PA
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)(2)(A)

Brief description of cause:
Data breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
Jun 14, 2024

SIGNATURE OF ATTORNEY OF RECORD
/s/ Gary F. Lynch

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DESIGNATION FORM
(to be used by counsel to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: 5907 Bridgeway Dr., Indian Trail, NC 28079; 4510 Jesse Bowman, San Antonio, TX 78253

Address of Defendant: 1020 Pattison Ave., Philadelphia, PA 19148; 334 South St., Philadelphia, PA 19147

Place of Accident, Incident or Transaction: 1020 Pattison Ave., Philadelphia, PA 19148; 334 South St., Philadelphia, PA 19147

RELATED CASE IF ANY:
Case Number:_____ Judge:_____ Date Terminated_____

Civil cases are deemed related when ***Yes*** is answered to any of the following questions:

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? Yes ☐ No ☒
2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit Pending or within one year previously terminated action in this court? Yes ☐ No ☒
3. Does this case involve the validity or infringement of a patent already in suit or any earlier Numbered case pending or within one year previously terminated action of this court? Yes ☐ No ☒
4. Is this case a second or successive habeas corpus, social security appeal, or pro se case filed by the same individual? Yes ☐ No ☒

I certify that, to my knowledge, the within case ☐ **is** / ☑ **is not** related to any now pending or within one year previously terminated action in this court except as note above.

DATE: 6/14/2024 /s/ Gary F. Lynch PA 56887

Attorney-at-Law (Must sign above) *Attorney I.D. # (if applicable)*

Civil (Place a √ in one category only)

A. Federal Question Cases:

- ☐ 1. Indemnity Contract, Marine Contract, and All Other Contracts)
- ☐ 2. FELA
- ☐ 3. Jones Act-Personal Injury
- ☐ 4. Antitrust
- ☐ 5. Wage and Hour Class Action/Collective Action
- ☐ 6. Patent
- ☐ 7. Copyright/Trademark
- ☐ 8. Employment
- ☐ 9. Labor-Management Relations
- ☐ 10. Civil Rights
- ☐ 11. Habeas Corpus
- ☐ 12. Securities Cases
- ☐ 13. Social Security Review Cases
- ☐ 14. Qui Tam Cases
- ☐ 15. All Other Federal Question Cases. *(Please specify)*:_____

B. Diversity Jurisdiction Cases:

- ☐ 1. Insurance Contract and Other Contracts
- ☐ 2. Airplane Personal Injury
- ☐ 3. Assault, Defamation
- ☐ 4. Marine Personal Injury
- ☐ 5. Motor Vehicle Personal Injury
- ☐ 6. Other Personal Injury (*Please specify*):_____
- ☐ 7. Products Liability
- ☒ 8. All Other Diversity Cases: *(Please specify)* data breach

ARBITRATION CERTIFICATION
(The effect of this certification is to remove the case from eligibility for arbitration)

I, Gary F. Lynch, counsel of record *or* pro se plaintiff, do hereby certify:

☒ Pursuant to Local Civil Rule 53.2 § 3(c)(2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of $150,000.00 exclusive of interest and costs:

☒ Relief other than monetary damages is sought.

DATE: 6/14/2024 /s/ Gary F. Lynch PA 56887

Attorney-at-Law (Sign here if applicable) *Attorney ID # (if applicable)*

NOTE: A trial de novo will be a jury only if there has been compliance with F.R.C.P. 38.