ROSSBACH LAW, P.C.
William A. Rossbach
401 North Washington Street
P.O. Box 8988
Missoula, MT 59807-8988
Phone: (406) 543-5156
bill@rossbachlaw.com

COTCHETT, PITRE & McCARTHY LLP
Thomas E. Loeser (pro hac vice forthcoming)
Karin B. Swope (pro hac vice forthcoming)
999 N. Northlake Way, Suite 215
Seattle, WA 98103
Tel: (206) 802-1272
Fax: (650) 697-0577
tloeser@cpmlegal.com.com
kswope@cpmlegal.com

Attorneys for Plaintiff Maddalena Bowers and the Proposed Class

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
BUTTE DIVISION

MADDALENA BOWERS, on behalf of herself and a class of similarly situated persons,

Plaintiff,

v.

SNOWFLAKE, INC.

Defendant.

NO.: CV-24-55-BU-JTJ

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

Plaintiff Maddalena Bowers, individually and on behalf of all others similarly situated ("Plaintiff"), brings this action against Defendant Snowflake, Inc. ("Snowflake" or "Defendant"), seeking monetary damages, restitution, and/or injunctive relief for the proposed Class, as defined below. Plaintiff makes the following allegations upon information and belief, the investigation of counsel, and personal knowledge or facts that are a matter of public record.

I. INTRODUCTION

1. The release, disclosure, and publication of sensitive, private data can be devastating. Not only is it an intrusion of privacy and a loss of control, but it is a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.[1] A data breach can have grave consequences for victims for years after the actual date of the breach—with the obtained information, thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, obtain government benefits, and/or obtain driver's licenses in the victims' names, forcing victims to maintain a constant vigilance over the potential misuse of their information.

2. This class action arises out of Snowflake's failure to secure its cloud storage systems, enabling criminals to access and misuse highly sensitive Private Information from Snowflake's cloud storage and systems that Plaintiff and

[1] Dave Maxfield & Bill Latham, Data Breaches: Perspectives from Both Sides of the Wall, S.C. Lawyer (May 2014).

members of the Class provided to companies that, in turn relied on Snowflake to store and protect such Private Information (the "Data Breach").

3. One of Defendant's customers was Beverly Hills, California based Ticketmaster, which is a wholly owned subsidiary of Live Nation and markets itself as a sophisticated, reliable entertainment ticket seller. Live Nation is "the largest live entertainment company in the world, connecting over 765 million fans across all of our concerts and ticketing platforms in 49 countries during 2023."[2] In its Privacy Policy found on its website, Live Nation has a section entitled "Looking After Your Information," under which it claims" "We take steps to try to make sure your information is protected and to delete it securely when we no longer need it."[3]

4. Despite these representations, Ticketmaster engaged Defendant Snowflake to manage its Data Cloud virtual warehouse, but protection of the information it maintains from and about its customers was woefully inadequate.

5. On May 29, 2024, Live Nation confirmed in a brief Form 8-k filing with the SEC that on May 20, 2024, it discovered that a third-party database containing its customers' private information had been breached. Specifically, the disclosure form stated:

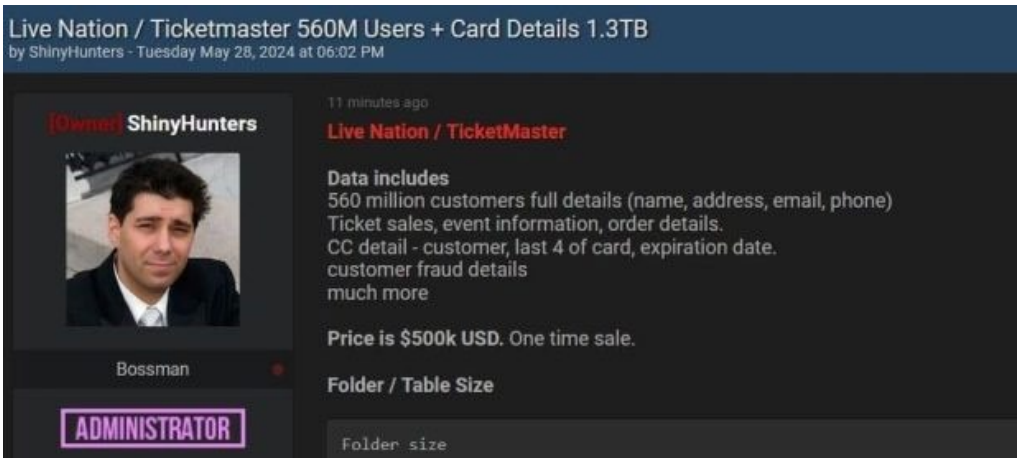
---

[2] Form 10-K Annual Report for Live Nation Entertainment, Inc., BAMSEC, https://www.bamsec.com/filing/133525824000017?cik=1335258 (last visited June 4, 2024).

[3] *Live Nation Privacy Policy*, LIVE NATION, available online at https://help.livenation.com/hc/en-us/articles/10464047306641-Live-Nation-Entertainment-Privacy-Policy#security (last visited June 4, 2024).

> On May 20, 2024, Live Nation Entertainment, Inc. (the "Company" or "we") identified unauthorized activity within a third-party cloud database environment containing Company data (primarily from its Ticketmaster L.L.C. subsidiary) and launched an investigation with industry-leading forensic investigators to understand what happened. On May 27, 2024, a criminal threat actor offered what it alleged to be Company user data for sale via the dark web. We are working to mitigate risk to our users and the Company, and have notified and are cooperating with law enforcement. As appropriate, we are also notifying regulatory authorities and users with respect to unauthorized access to personal information.[4]

6. On or around May 28, 2024, the Private Information of 560,000,000 Ticketmaster and Live Nation's customers was compromised and listed for sale.[5] The notorious hacker group known only by its alias "ShinyHunters" claimed that it had stolen 1.3 terabytes of personal data and is reportedly ready to sell, or has



[4] *Id.*

[5] Georgie Hewson, *Home Affairs Department confirms cyber incident impacting Ticketmaster customers*, ABC NEWS (May 29, 2024), https://www.abc.net.au/news/2024-05-29/ticketmaster-hack-allegedlyshinyhunter-customers-data-leaked/103908614. (last visited July 3, 2024).

already sold, such information to nefarious dark web users for $500,000, as illustrated by their post on BreachForums, a dark-web marketplace for stolen data.

7. This Data Breach occurred because Snowflake enabled an unauthorized third party to gain access to and obtain former and current Ticketmaster and Live Nation's customers' Private Information from Ticketmaster's systems housed by Snowflake.[6]

8. Ticketmaster and Live Nation store customer data in a virtual warehouse provided by Defendant Snowflake, which offers its "Data Cloud" to institutional customers to consolidate and store data.[7]

9. Snowflake provides digital warehouses, known as "Snowflake Data Clouds," for its thousands of clients around the world, and as a result has access to, stores, and maintains huge datasets of Private Information of its corporate clients' customers and employees. For the purposes of this action, Snowflake's corporate clients are entities that contracted with Snowflake to store confidential files of their customers and employees. Snowflake's corporate clients include, but are not limited to, AT&T, Ticketmaster, Mastercard, Nielsen, Novartis, PepsiCo, Siemens, Advanced Auto Parts, Santander Bank, Allstate Insurance, Anheuser-Busch,

[6] *Id.*

[7] *Form 10-K Annual Report for Snowflake, Inc.*, BAMSEC, https://www.bamsec.com/filing/164014724000101?cik=1640147 (last visited July 3, 2024).

Mitsubishi, Neiman Marcus, Doordash, HP, Instacart, Capital One, JetBlue, Pitney Bowes, Progressive, State Farm, NBC Universal, and many others.[8]

10. As a result of the Data Breach, through which their Personally Identifiable Information ("PII") was compromised, disclosed, and obtained by unauthorized third parties, Plaintiff and Class Members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud and identity theft for a period of years, if not decades. Furthermore, Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft, at their own expense. Consequently, Plaintiff and the other Class Members will incur ongoing out-of-pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

11. By this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

II. JURISDICTION, VENUE, AND CHOICE OF LAW

12. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711, *et seq.*, because at least one member of the Class, as

[8] *See* Leaders Choose Snowflake, SNOWFLAKE (N.D.), https://www.snowflake.com/en/customers/all-customers/ (las accessed July 8, 2024).

defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs. This Court also has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a).

13. Defendant Snowflake is subject to personal jurisdiction in Montana as a resident of this state. Defendant Snowflake is authorized to do and is doing business, advertises, and solicits business within the state. By residing in Montana, Defendant is physically present and subject to its laws.

14. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Snowflake's principal place of business is located in this District and a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

III. PARTIES

A. Plaintiff Maddalena Bowers

15. Plaintiff Maddalena Bowers is a citizen of and is domiciled in Torrance in the state of California.

16. Plaintiff is a customer of Ticketmaster and has purchased, on average, 15-20 sets of tickets from Ticketmaster for various events.

17. Plaintiff provided confidential and sensitive PII to Ticketmaster, as requested and required by Ticketmaster for the provision of its services. Ticketmaster obtained and through Defendant Snowflake continues to maintain

Plaintiff's PII and Snowflake has a legal duty and obligation to protect that PII from unauthorized access and disclosure.

18. Plaintiff would not have entrusted her PII to Ticketmaster had she known that Ticketmaster would provide it to Snowflake, which failed to maintain adequate data security.

19. On or about June 27, 2024, Plaintiff read online about the Data Breach. She learned that Ticketmaster had lost the information of 560 million customers. Because Plaintiff regularly purchases 15-20 set of tickets from Ticketmaster each year, on information and belief, Plaintiffs information is included among the 560 million customer records that were compromised from Snowflake's systems and offered for sale on the Dark Web.

20. Plaintiff subsequently spent several hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect herself from data breaches, and reviewing her financial accounts for fraud or suspicious activity. She now plans to spend several hours a month checking account statements for irregularities.

21. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of her PII, which she expected Defendant to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using her PII. As a result of the Data Breach,

Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

B. Defendant

22. Defendant Snowflake, Inc. is a Delaware corporation headquartered in Montana with its principal executive office located at 106 E. Babcock, Suite A Bozeman, MT 59715.

23. Snowflake is a publicly traded corporation listed on the New York Stock Exchange with revenues totaling approximately $829 million for the three months ended on April 30, 2024.[9]

24. Snowflake's Data Cloud platform is used globally, with 9,437 institutions trusting Snowflake to manage and store customers' data.[10]

25. Due to the nature of the services Snowflake provides, it receives and is entrusted with securely storing consumers' Private Information, which includes, inter alia, individuals' full name, payment information, occasional location data, and other sensitive information. As a contracting party entrusted with millions of customers' PII, Snowflake was expected to provide confidentiality and adequate security for the data it collected in accordance with Defendant Ticketmaster's

[9] *Form 10-Q Quarterly Report for Snowflake, Inc.*, BAMSEC, https://www.bamsec.com/filing/164014724000135?cik=1640147 (last visited June 12, 2024).

[10] *Form 10-K Annual Report for Snowflake, Inc.*, BAMSEC, https://www.bamsec.com/filing/164014724000101?cik=1640147 (last visited June 12, 2024).

promises and disclosures and is expected to comply with statutory privacy requirements.

26. In the course of its business, Ticketmaster collects names, phone numbers, Social Security numbers, physical addresses, driver's license information, and other information from its customers and prospective customers and it stores and maintains this information in Snowflake's cloud computing system and storage.

IV. FACTUAL BACKGROUND

A. Defendant Failed to Adequately Protect Customer Data, Resulting in the Data Breach

27. On May 28, 2024, ShinyHunters, a known criminal hacking group, posted for sale 1.3 terabytes of PII on a hacker forum and marketplace.[11] According to ShinyHunters' forum post, the PII included "560 million customers [*sic*] full details (name, address, email, phone) [¶] Ticket sales, event information, order details [¶] CC [credit card] detail [*sic*] [¶] customer, last 4 of card, expiration date. Customer fraud details [¶] much more."[12] ShinyHunters offered to sell the data for $500,000.[13]

[11] Waqas, *Hackers Claim Ticketmaster Data Breach: 560M Users' Info for Sale at $500k*, HACKREAD (June 3, 2024), https://hackread.com/hackers-ticketmaster-data-breach- 560m-users-sale/.

[12] *Id.*

[13] *Id.*

28. On May 29, 2024, Live Nation made a Form 8-k filing with the SEC reporting that on May 20, 2024, it discovered that its customers' private information had been offered for sale. The disclosure stated that Live Nation had "identified unauthorized activity within a third-party cloud database environment containing Company data (primarily from its Ticketmaster L.L.C. subsidiary) and launched an investigation with industry-leading forensic investigators to understand what happened."[14] The disclosure further stated that Live Nation was "working to mitigate risk to our users and the Company[.]"[15]

29. Snowflake is familiar with its obligations—created by contract, industry standards, common law, and representations to their customers—to protect customer information. Plaintiff and Class Members provided their PII to Ticketmaster and other Snowflake clients with the reasonable expectation that any company entrusted with their information would comply with its obligations to keep such information confidential and secure.

30. Ticketmaster states on its website: "We're always taking steps to make sure your information is protected and deleted securely" and "[w]e have security measures in place to protect your information."[16]

[14] *See* Form 8-k, attached as Exhibit A.

[15] *Id.*

[16] *Privacy Policy*, TICKETMASTER, https://privacy.ticketmaster.com/privacy-policy (last visited June 4, 2024).

31. Ticketmaster also sets forth "10 commitments" on its website, including its purported commitment to "Security & Confidentiality."[17] Specifically, Ticketmaster asserts that "[t]he security of our fans' information is a priority for us. We take all necessary security measures to protect personal information that's shared and stored with us."[18]

32. Snowflake knew that its customers were relying on it to comply with their promises concerning data security, yet failed to comply with these obligations, resulting in the Data Breach. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records.

B. Defendant's Lack of Security for its Data Environment

33. As a direct result of Snowflake's failure to implement basic security measures, millions of Americans have had their PII made available on the dark web to be purchased by criminals. Cybersecurity firms, journalists, and threat actors have claimed that 165 Snowflake customers' data had been exfiltrated. At least the confidential customer data of the following companies have been released as a result of Snowflake's failure to secure its customers' customer information:[19]

- **Ticketmaster**. On May 28, 2024, threat actors posted that 1.4

[17] *Our Commitments*, TICKETMASTER, https://privacy.ticketmaster.com/en/our-commitments (last visited June 4, 2024).

[18] *Id.*

[19] *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, MANDIANT (June 10, 2024), https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion (last accessed July 8, 2024).

terabytes of Ticketmaster customers' Private Information was available for purchase on the hacking website Breach Forums.[20] The notorious hacking group ShinyHunters offered the trove of Plaintiff's and Class Members' Private Information for $500,000. Ticketmaster has confirmed the loss of files was a result of Snowflake's Data Breach which occurred on May 20, 2024.[21] The lost information included "560 million customers [sic] full details (name, address, email, phone) – Ticket sales, event information, order details – CC [credit card] detail [sic] – customer, last 4 of card, expiration date. Customer fraud details – much more."

- **Advance Auto Parts**. Likewise, the Data Breach also affected the employees and customers of Advanced Auto parts. The released information included sensitive employee data. On June 5, 2024, the threat actor known by their online handle "Sp1d3r," posted on a hacking forum that 3 Terabytes of AAP's data was up for sale. The hacker confirmed that the data was exfiltrated from "AAP Snowflake" and included: "380M customer profiles (name, email, mobile, phone, address, more) – 140M customer orders – 44M Loyalty/Gas card

[20] Waqas, *supra,* Note 12. (last accessed July 8, 2024).

[21] Form 8-K Current Report for Live Nation Entertainment, Inc., SEC.GOV, https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm?=7194ef805fa2d04b0f7e8c9521f97343 (last accessed July 8, 2024).

numbers (with customer details) – 358K Employees – Sales history – Employment candidate info with SSNs, drivers' license numbers, demographic details – Transaction tender details – Over 200 tables of data!"[22] This trove of information is available for $1.5 million USD.

- **Neiman Marcus**. As a result of Snowflake's failure to protect information, its customers – clients of Neiman Marcus, stored on its data cloud, were also affected. Spid3r posted their sensitive information for sale, confirming that names, emails, addresses, dates of birth, last four digits of social security numbers, 50 million customer emails and IP addresses, and 70 million customer transaction data were included in this dataset.[23] Neiman Marcus so far has confirmed that only 64,472 people were impacted, which appears to be incorrect, given the size of the data set for sale.
- **Lending Tree**. As a result of Snowflake's failure to protect Private Information, customers of Snowflake client Lending Tree were also affected. Sp1d3r confirmed that it exfiltrated 190 million customers' personal data and "3 billion pixel data" including "full customer

[22] Sergiu Gatlan, *Advance Auto Parts Stolen Data For Sale After Snowflake Attack*, BLEEPINGCOMPUTER (June 5, 2024) https://www.bleepingcomputer.com/news/security/advance-auto-parts-stolen-data-for-sale-after-snowflake-attack/ (last accessed July 8, 2024).

[23] Lawrence Abrams, *Neiman Marcus Confirms Data Breach After Snowflake Account Hack*, BLEEPINGCOMPUTER (June 28, 2024), https://www.bleepingcomputer.com/news/security/neiman-marcus-confirms-data-breach-after-snowflake-account-hack/ (last accessed July 8, 2024).

details, partial CC details (only middle 5 numbers masked), auto history, driving records, personal background information needed for insurance quotes, 3 billion tracking pixels (contains PII and IP/online tracking details." Sp1d3r furthered sweetened its trove of data by including some of Lending Tree's subsidiary's (QuoteWizard) clients, which include the largest auto insurance companies in the United States, such as Allstate, State Farm, Progressive and Farmers Insurance.[24]

C. Defendant Failed to Comply with FTC Guidelines

34. Defendant is prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

35. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

[24] Jonathan Greig, *LendingTree Confirms That Cloud Services Attack Potentially Affected Subsidiary*, THE RECORD (June 10, 2024), https://therecord.media/lendingtree-quotewizard-cybersecurity-incident-snowflake (last accessed July 8, 2024).

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

36. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[25] 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.[26]

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

[25] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited June 12, 2024).

[26] *Id.*

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

39. Defendant failed to properly implement basic data security practices, allowing for this attack to occur, victimizing hundreds of millions of people.

40. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

41. Defendant was at all times fully aware of the obligation to protect the Private Information of consumers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

42. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity and Infrastructure Security Agency, State Attorney General Offices and many other government and law enforcement agencies, and hundreds of private cybersecurity and threat intelligence firms, have issued warnings that put Defendant on notice, long before the Data Breach, that 1) cybercriminals are

targeting large, public companies such as Defendant Snowflake; 2) cybercriminals were ferociously aggressive in their pursuit of large collections of PII like that in possession of Defendant; 3) cybercriminals were selling large volumes of PII and corporate information on Dark Web portals; 4) the threats were increasing.

43. Had Defendant been diligent and responsible, it would have known about and acted upon warnings published in 2017 that 93% of data security breaches were avoidable and the key avoidable causes for data security incidents are:

a) Lack of complete assessment, including internal, third-party, and cloud-based systems and services;

b) Not promptly patching known/public vulnerabilities, and not having a way to process vulnerability reports;

c) Misconfigured devices/servers;

d) Unencrypted data and/or poor encryption key management and safeguarding;

e) Use of end-of-life (and thereby unsupported) devices, operating systems and applications;

f) Employee errors and accidental disclosures — lost data, files, drives, devices, computers, improper disposal;

g) Failure to block malicious email; and

h) Users succumbing to business email compromise (BEC) and social exploits.[27]

D. The Data Breach Puts Consumers at Increased Risk of Fraud and Identity Theft

44. An identity thief uses victims' PII, such as name, address, and other sensitive and confidential information, without permission, to commit fraud or other crimes that range from immigration fraud, obtaining a driver's license or identification card, obtaining government benefits, and filing fraudulent tax returns to obtain tax refunds.

45. Identity thieves can use a victim's PII to open new financial accounts, incur charges in the victim's name, take out loans in the victim's name, and incur charges on existing accounts of the victim. Plaintiff' finances are now at risk due to the Data Breach.

46. Identity theft is the most common consequence of a data breach—it occurs to 65% of data breach victims.[28] Consumers lost more than $56 billion to identity theft and fraud in 2020, and over 75% of identity theft victims reported emotional distress.[29]

---

[27] Gretel Egan, *OTA Report Indicates 93% of Security Breaches Are Preventable*, PROOFPOINT (Feb. 7, 2018), available at https://www.proofpoint.com/us/securityawareness/post/ota-report-indicates-93-security-breaches-are-preventable (last visited July 3, 2024).

[28] Eugene Bekker, *What Are Your Odds of Getting Your Identity Stolen?*, IDENTITYFORCE (Apr. 15, 2021), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics (last visited Feb. 1, 2023).

[29] *Id.*

47. Plaintiff is now in the position of having to take steps to mitigate the damages caused by the Data Breach. Once use of compromised non-financial PII is detected, the emotional and economic consequences to the victims are significant. Studies done by the ID Theft Resource Center, a non-profit organization, found that victims of identity theft had marked increased fear for personal financial security. The report attributes this to more people having been victims before, contributing to greater awareness and understanding that they may suffer long term consequences from this type of crime.[30]

48. Defendant failed to protect and safeguard Plaintiff's and Class Members' private information, in fact failing to adhere to even its most basic obligations. As a result, Plaintiff and Class Members have suffered or will suffer actual injury, including loss of privacy, costs, and loss of time.

V. CLASS ACTION ALLEGATIONS

49. Plaintiff brings this action as a class action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of a proposed nationwide class (the "Class"), defined as:

> All natural persons in the United States whose Personally Identifiable Information was compromised as a result of the Data Breach.

[30] Identity Theft: The Aftermath 2013, Identity Theft Resource Center, https://idtheftinfo.org/latest-news/72 (last visited Feb. 1, 2023).

50. In addition, the State Subclass is defined as follows:

> **California Subclass:** All natural persons in the State of California whose Personally Identifiable Information was compromised as a result of the Data Breach.

51. **Numerosity and Ascertainability:** Plaintiff does not know the exact size of the Class or identity of the Class Members, since such information is in the exclusive control of Defendant. Nevertheless, the Class, on information and belief includes millions of individuals dispersed throughout the United States, considering approximately 560 million Ticketmaster customers' information was reportedly subject to unauthorized access. The number of Class Members is so numerous that joinder of all Class Members is impracticable. The names, addresses, and phone numbers of Class Members are identifiable through documents maintained by Defendant.

52. **Commonality and Predominance:** This action involves common questions of law and fact which predominate over any question solely affecting individual Class Members. These common questions include:

A. whether Defendant engaged in the conduct alleged herein;

B. whether Defendant had a legal duty to use reasonable security measures to protect Plaintiff's and Class Members' PII;

C. whether Defendant timely, accurately, and adequately

informed Plaintiff and Class Members that their PII had been compromised;

D. whether Defendant breached its legal duty by failing to protect the PII of Plaintiff and Class Members;

E. whether Defendant acted reasonably in securing the PII of Plaintiff and Class Members;

F. whether Plaintiff and Class Members are entitled to injunctive relief;

G. and whether Plaintiff and Class Members are entitled to damages and equitable relief.

53. **Typicality:** Plaintiff's claims are typical of the other Class Members' claims because all Class Members were comparably injured through Defendant's substantially uniform misconduct, as described above. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other members of the Class that she represents, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and Class Members arise from the same operative facts and are based on the same legal theories.

54. **Adequacy:** Plaintiff is an adequate Class representative because her interests do not conflict with the interests of the other members of the Class she seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; and Plaintiff intends to prosecute this action

vigorously. The Class's interest will be fairly and adequately protected by Plaintiff and her counsel.

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

VI. CAUSES OF ACTION

A. Claims Brought on Behalf of the Nationwide Class

COUNT ONE
NEGLIGENCE

56. Plaintiff incorporates all foregoing factual allegations as if fully set forth herein.

57. Defendant owed a duty to Plaintiff and Class Members, arising from the sensitivity of the information, the expectation the information was going to be kept private, and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' information was adequately secured from unauthorized access.

58. Defendant owed a duty to Plaintiff and Class Members to implement administrative, physical and technical safeguards, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiff's and Class Members' PII.

59. Defendant also had a duty to only maintain PII that was needed to serve customer needs.

60. Defendant owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Plaintiff's and Class Members' PII.

61. Defendant also had independent duties under Plaintiff's and Class Members' state laws that required Ticketmaster to reasonably safeguard Plaintiff's and Class Members' PII, and promptly notify them about the Data Breach.

62. Ticketmaster had a special relationship with Plaintiff and Class Members as a result of being entrusted with their PII, which provided an independent duty of care. Plaintiff's and Class Members' willingness to entrust Ticketmaster and other Snowflake clients with their PII was predicated on the understanding that these companies and their vendor, Snowflake, would take adequate security precautions. Moreover, Defendant was capable of protecting its networks and systems, and the PII it stored on them, from unauthorized access.

63. Defendant breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Plaintiff's and Class Members' PII, including administrative, physical, and technical safeguards; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that its data security practices were inadequate to safeguard Plaintiff's and Class Members' PII.

64. But for Defendant's breach of duties, including the duty to use reasonable care to protect and secure Plaintiff's and Class Members' PII,

Plaintiff's and Class Members' PII would not have been accessed by unauthorized parties.

65. Plaintiff and Class Members were foreseeable victims of Defendant's inadequate data security practices. Defendant knew or should have known that a breach of its data security systems would cause damage to Plaintiff and Class Members.

66. It was reasonably foreseeable that the failure to reasonably protect and secure Plaintiff's and Class Members' PII would result in unauthorized access to Defendant's networks, databases, and computers that stored or contained Plaintiff's and Class Members' PII.

67. As a result of Defendant's negligent failure to prevent the Data Breach, Plaintiff and Class Members suffered injury, which includes, but is not limited to, exposure to a heightened and imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiff and Class Members have also incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter and detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII has also diminished the value of the PII.

68. The harm to Plaintiff and Class Members was a proximate, reasonably foreseeable result of Defendant's breaches of its aforementioned duties.

69. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT TWO
NEGLIGENCE PER SE

70. Plaintiff incorporates all foregoing factual allegations as if fully set forth herein.

71. Under the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

72. In addition, under state data security statutes, Defendant had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' PII.

73. Defendant breached its duties to Plaintiff and Class Members, under the Federal Trade Commission Act, 15 U.S.C. § 45, ("FTCA") and the state data security statutes, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

74. Plaintiff and Class Members were foreseeable victims of Defendant's violations of the FTCA and state data security statutes. Defendant knew or should

have known that its failure to implement reasonable measures to protect and secure Plaintiff's and Class Members' PII would cause damage to Plaintiff and Class Members.

75. Defendant's failure to comply with the applicable laws and regulations constitutes negligence *per se.*

76. But for Defendant's violation of the applicable laws and regulations, Plaintiff's and Class Members' PII would not have been accessed by unauthorized parties.

77. As a result of Defendant's failure to comply with applicable laws and regulations, Plaintiff and Class Members suffered injury, which includes but is not limited to the exposure to a heightened and imminent risk of fraud, identity theft, financial and other harm. Plaintiff and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiff and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII has also diminished the value of the PII.

78. The harm to Plaintiff and the Class Members was a proximate, reasonably foreseeable result of Defendant's breaches of the applicable laws and regulations.

79. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT THREE
BREACH OF FIDUCIARY DUTY

80. Plaintiff incorporates all foregoing factual allegations as if fully set forth herein.

81. Plaintiff and Class Members either directly or indirectly gave Defendant their Private Information in confidence, believing that Defendant would protect that information. Plaintiff and Class Members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiff's and Class Members' Private Information created a fiduciary relationship between Defendant and Plaintiff and Class Members. Considering this relationship, Defendant must act primarily for the benefit of Plaintiff and Class Members, which includes safeguarding and protecting Plaintiff's and Class Members' Private Information.

82. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' Private Information, failing to safeguard the Private Information of Plaintiff and Class Members it collected.

83. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT FOUR
UNJUST ENRICHMENT

84. Plaintiff realleges and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

85. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of monetary payments—directly or indirectly—for services received.

86. Defendant collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant had knowledge of the monetary benefits conferred by Plaintiff and Class Members.

87. The money that Plaintiff and Class Members paid to Defendant indirectly through Defendant's clients should have been used to pay, at least in part, for the administrative costs and implementation of data management and security. Defendant failed to implement—or adequately implement—practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

88. As a result of Defendant's failure to implement security practices, procedures, and programs to secure sensitive PII, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in the value between services with reasonable data privacy that Plaintiff and Class Members paid for, and the services they received without reasonable data privacy.

89. Under principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members because Defendant failed to implement the data management and security measures that are mandated by industry standards and that Plaintiff and Class Members paid for.

90. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by Defendant. A constructive trust should be imposed upon all unlawful and inequitable sums received by Defendant traceable to Plaintiff and the Class.

COUNT FIVE
DECLARATORY JUDGMENT

91. Plaintiff realleges and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

92. Plaintiff and the Class have stated claims against Defendant based on negligence, negligence per se, gross negligence and negligent misrepresentation, and violations of various state and federal statutes.

93. Defendant failed to fulfill their obligations to provide adequate and reasonable security measures for the PII of Plaintiff and the Class, as evidenced by the Data Breach.

94. As a result of the Data Breach, Defendant's system is more vulnerable to unauthorized access and requires more stringent measures to be taken to safeguard the PII of Plaintiff and the Class going forward.

95. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's current obligations to provide reasonable data security measures to protect the PII of Plaintiff and the Class. Defendant maintains that its security measures were—and still are— reasonably adequate and denies that it previously had or has any obligation to implement better safeguards to protect the PII of Plaintiff and the Class.

96. Plaintiff seeks a declaration that Defendant must implement specific additional, prudent industry security practices to provide reasonable protection and

security to the PII of Plaintiff and the Class. Specifically, Plaintiff and the Class seek a declaration that Defendant's existing security measures do not comply with their obligations, and that Defendant must implement and maintain reasonable security measures on behalf of Plaintiff and the Class to comply with their data security obligations.

B. Claims Brought on Behalf of the California Subclass

COUNT SIX
VIOLATION OF THE
CALIFORNIA CUSTOMER RECORDS ACT,
CAL. CIV. CODE §§ 1798.80, *ET SEQ*.

97. Plaintiff Bowers ("Plaintiff" for purposes of this claim), individually and on behalf of the California Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach.

98. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the

Personal Information from unauthorized access, destruction, use, modification, or disclosure."

99. Defendant is a business that owns, maintains, and licenses "personal information", within the meaning of Cal. Civ. Code § 1798.81.5(d)(1), about Plaintiff and California Subclass members.

100. On information and belief, Snowflake is registered as a "data broker" in California, which is defined as a "business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80.[31]

101. Businesses that own or license computerized data that includes personal information, including SSNs, are required to notify California residents when their personal information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

102. Defendant is a business that own or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82(h).

[31] https://oag.ca.gov/data-broker/registration/185724.

103. Plaintiff and California Subclass members' Private Information includes "personal information" as covered by Cal. Civ. Code §§ 1798.81.5(d)(1), 1798.82(h).

104. Because Defendant reasonably believed that Plaintiff and California Subclass members' Private Information was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

105. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Cal. Civ. Code § 1798.82.

106. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above.

107. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT SEVEN
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *ET SEQ.*

108. Plaintiff Bowers ("Plaintiff" for purposes of this claim), individually and on behalf of the California Subclass, incorporates all foregoing factual allegations as if fully set forth herein.

109. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach.

110. Defendant is a "person" as defined by Cal. Bus. & Prof. Code §17201.

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

112. Defendant's "unfair" and "deceptive" acts and practices include:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and the California Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f) Failing to timely and adequately notify Plaintiff and the California Subclass Members of the Data Breach;

g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and the California Subclass Members' Private Information; and

h) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

113. Defendant has engaged in "unlawful" business practices by violating multiple laws, including the CCRA, Cal. Civ. Code §§ 1798.80, *et seq.*, the CLRA, Cal. Civ. Code §§ 1780, *et seq.*, 15 U.S.C. § 680, *et seq.,* the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

114. Defendant's unlawful practices include:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq*., HIPAA, 42 U.S.C. § 1320d., COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the Data Breach;

d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and the California Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801,

et seq., HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501- 6505, and the CMIA, Cal. Civ. Code § 56.36(b);

f) Failing to timely and adequately notify the Plaintiff and the California Subclass Members of the Data Breach;

g) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and the California Subclass Members' Private Information; and

h) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the California Subclass Members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq*., HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

115. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

116. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the California Subclass members, into believing that their Private Information was secure.

117. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, including monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information, including, but not limited to, the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

118. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff and California Subclass members' rights.

119. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT EIGHT
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT, CAL. CIV. CODE §§ 1798.100, *ET SEQ.*

120. Plaintiff Bowers ("Plaintiff" for purposes of this claim), individually and on behalf of the California Subclass, incorporates all foregoing factual allegations as if fully set forth herein.

121. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach.

122. Plaintiff and California Subclass members are residents of California.

123. Defendant is a corporation that is organized or operated for the profit or financial benefit of its shareholders or other owners.

124. Defendant is a business that collects consumers' personal information as defined by Cal. Civ. Code § 1798.140(e). Specifically, Defendant obtains, receives, or accesses consumers' personal information when customers sign up with companies that use Defendant's service.

125. On information and belief, Defendant is registered as a "data broker" in California, which is defined as a "business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80.

126. Defendant violated Section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiff and the California Subclass members' nonencrypted and nonredacted personal information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

127. Defendant knew or should have known that its data security practices were inadequate to secure the California Subclass members' Private Information and that its inadequate data security practices gave rise to the risk of a data breach.

128. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the Private Information it collected and stored.

129. Upon information and belief, Plaintiff and California Subclass members' Private Information accessed by the cybercriminals in the Data Breach includes "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d).

130. Plaintiff seeks injunctive relief in the form of an order requiring Defendant to employ adequate security practices consistent with law and industry standards to protect the California Subclass members' Private Information, requiring Defendant to complete its investigation, and to issue an amended statement giving a detailed explanation that confirms, with reasonable certainty,

what categories of data were stolen and accessed without the California Subclass members' authorization, along with an explanation of how the data breach occurred.

131. Plaintiff and the California Subclass members seek statutory damages or actual damages, whichever is greater, pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

132. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.150, Plaintiff and California Subclass members suffered damages, as described above.

133. Plaintiff and the California Subclass seek pecuniary damages pursuant to Cal. Civil Code § 1798.150(b).

VII. PRAYER FOR RELIEF

Plaintiff, on behalf of herself and on behalf of the proposed Class and Subclass, requests that the Court:

a. Certify this case as a class action, appoint Plaintiff as class representatives, and appoint Plaintiff's Counsel as Class Counsel for Plaintiff to represent the Class;

b. Find that Defendant breached its duty to safeguard and protect the PII of Plaintiff and Class Members that was compromised in the Data Breach;

c. Award Plaintiff and Class Members appropriate relief, including

actual and statutory damages, restitution and disgorgement;

d. Award equitable, injunctive and declaratory relief as may be appropriate;

e. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

f. Award pre-judgment and post-judgment interest as prescribed by law; and

g. Grant additional legal or equitable relief as this Court may find just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

DATED this 10th day of July, 2024.

ROSSBACH LAW, P.C.

/s/ William A. Rossbach
William A. Rossbach

COTCHETT PITRE & MCCARTHY LLP

Thomas E. Loeser (*pro hac vice to be filed*)
Karin B. Swope (*pro hac vice to be filed)*
Attorneys for Plaintiff Maddalena Bowers and the proposed Class